Universität Hamburg
Fachbereich Informatik

Studienarbeit

Anonymisierung von Internet-Diensten

Ulf Möller
<3umoelle@informatik.uni-hamburg.de>

12. Januar 1998

Betreuer: Prof. Dr. K. Brunnstein

Inhaltsverzeichnis

Abkürzungsverzeichnis

AWG	Außenwirtschaftsgesetz
BDSG	Bundesdatenschutzgesetz
GG	Grundgesetz
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IuKDG	Informations- und Kommunikationsdienstegesetz
MAC	Message Authentication Code
MDStV	Mediendienste-Staatsvertrag
MIME	Multipurpose Internet Mail Extensions
PGP	Pretty Good Privacy
SigG	Signaturgesetz
S/MIME	Secure MIME
SSH	Secure Shell
SSL	Secure Socket Layer
StPO	Strafprozeßordnung
TCP	Transmission Control Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikationsdienstunternehmen-Datenschutzverordnung
TKG	Telekommunikationsgesetz
URL	Uniform Resource Locator
WWW	World Wide Web

Kapitel 1

Einleitung

Seit Beginn der 90er Jahre erlebt das Internet ein explosives Wachstum. Das im wissenschaftlichen Umfeld entstandene Kommunikationsnetz gewinnt zunehmend Bedeutung für Privatpersonen und Wirtschaft; diese Entwicklung wird häufig als Beginn des Wandels von der Produktions- zu einer Informationsgesellschaft angesehen. Der deutsche Gesetzgeber sah die Notwendigkeit, diesen Wandel durch das *Informations- und Kommunikationsdienstegesetz* aktiv zu gestalten.

Den erweiterten Risiken für die informationelle Selbstbestimmung in globalen Netzen soll eine den Datenschutz gewährleistende technische Infrastruktur entgegengesetzt werden [Bundestag 1997]. Dabei gilt der Grundsatz, das Entstehen personenbezogener Daten zu vermeiden, indem den Nutzern anonymes Handeln ermöglicht wird.

In dieser Arbeit sollen Verfahren, die eine anonyme Nutzung von Netzdiensten ermöglichen, in Bezug auf ihre Sicherheit und Effizienz untersucht und Anwendungsmöglichkeiten im Internet betrachtet werden.

Kapitel 2

Rechtliche Grundlagen

2.1 Datenschutz in globalen Netzen

Das Entstehen einer weltweiten Informationsinfrastruktur bereitet für den Datenschutz besondere Probleme. Da immer mehr Vorgänge des alltäglichen Lebens elektronisch abgewickelt werden, steigt die Menge der personenbezogenen Daten, die gespeichert und analysiert werden können. Zudem können Informationen aufgrund der Vernetzung und neuer Techniken der Datenauswertung in bisher ungekannter Weise ausgewertet werden; Datenschutzvorschriften lassen sich im weltweiten Netz kaum noch durchsetzen. Statt dessen muß der verfassungsrechtlich erforderliche Datenschutz mit technischen Mitteln gewährleistet werden.

2.1.1 Den Datenschutz betreffende Gesetze

Die Privatsphäre und die Selbstbestimmung über Informationen werden vom Grundgesetz gewährleistet. Art. 10 GG schützt das Brief-, Post- und Fernmeldegeheimnis. Das Recht auf informationelle Selbstbestimmung ist aus dem allgemeinen Persönlichkeitsrecht (Art. 1 und 2 GG) abgeleitet. Die daraus resultierenden Anforderungen werden durch verschiedene einfache Gesetze umgesetzt.

Das Telekommunikationsgesetz (TKG) verpflichtet Erbringer von Telekommunikationsdienstleistungen zur Einhaltung des Fernmeldegeheimnisses.

Die informationelle Selbstbestimmung und die Verarbeitung personenbezogener Daten werden durch das BDSG und die Landesdatenschutzgesetze sowie durch bereichsspezifisches Datenschutzrecht geregelt. Im Bereich der Telekommunikation regeln das TKG und die TDSV den Datenschutz.

Regelungen über elektronische Informations- und Kommunikationsdienste treffen das Informations- und Kommunikationsdienstegesetz [IuKDG 1997] und der Mediendienste-Staatsvertrag der Bundesländer [MDStV 1997]. Das in der Entwurfsphase unter dem Titel „Multimedia-Gesetz“ bekannt gewordene IuKDG gilt für individuell nutzbare Dienste (Teledienste), der MDStV für an die Allgemeinheit gerichtete Dienste (Mediendienste). Das IuKDG besteht aus dem Teledienstegesetz (TDG), dem Teledienstedatenschutzgesetz (TDDSG), dem Signaturgesetz (SigG) und Änderungen weiterer Gesetze.

Die Unterscheidung zwischen zwischen Telediensten und Mediendiensten ist durch die unterschiedlichen Zuständigkeiten von Bund und Ländern bedingt. Die Abgrenzung ist nicht immer eindeutig; allerdings enthalten IuKDG und MDStV weitgehend identische Datenschutzbestimmungen.

Das Datenschutzrecht anderer Staaten unterscheidet sich vom deutschen teilweise erheblich. Während der Datenschutzrichtlinie der Europäischen Union vergleichbare Prinzipien zugrunde liegen, hat in den USA die Transparenz staatlichen Handelns einen höheren Stellenwert. In dieser Arbeit soll auf die Rechtslage außerhalb Deutschlands nur insoweit eingegangen werden, wie sie aufgrund der globalen Vernetzung unmittelbare Auswirkungen auf Deutschland hat.

2.1.1.1 Das Recht auf informationelle Selbstbestimmung

Jeder hat das Recht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Dieses Recht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht aus dem vom Grundgesetz geschützten allgemeinen Persönlichkeitsrecht abgeleitet: Mit Hilfe der automatischen Datenverarbeitung können personenbezogene Daten unbegrenzt gespeichert, jederzeit abgerufen und Daten aus verschiedenen Quellen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild verknüpft werden, über dessen Verwendung der Betroffene keine hinreichende Kontrolle hat. Schon der psychische Druck durch die so möglich werdende öffentliche Anteilnahme kann auf das Verhalten des einzelnen einwirken und ihn in der tatsächlichen Wahrnehmung seines Selbstbestimmungsrechts einschränken. Wer nicht weiß, welche Informationen über ihn von wem gespeichert werden, kann die Konsequenzen seines Handelns nicht zuverlässig überblicken und wird möglicherweise auf die Ausübung seiner Grundrechte verzichten, um nicht durch abweichende Verhaltensweisen aufzufallen [BVerfG 1983, S. 42f].

Diese Gefahr besteht auch für die kommunikative Selbstbestimmung. Um anderen als Kommunikationspartner gegenübertreten zu können, muß der einzelne das Wissen des anderen und damit die eigene Situation korrekt abschätzen können. Wer nicht selbst darüber entscheiden kann, unter welchen Voraussetzungen und mit welchen Zielen andere Zugang zu den ihn charakterisierenden Daten erhalten, läuft Gefahr, nicht mehr als Subjekt am Kommunikationsprozeß teilnehmen zu können und zunehmend zum Adressaten von Verhaltenserwartungen zu werden [Simitis 1992, § 1 Rdnr. 169].

Damit wären aber nicht nur die individuellen Entfaltungschancen des einzelnen gefährdet, sondern ebenso das demokratische Gemeinwesen, das auf der Handlungs- und Mitwirkungsfähigkeit seiner Bürger beruht [BVerfG 1983, S. 43].

Der Betroffene muß die Folgen der Datenverarbeitung somit möglichst genau überblicken können. Daher sind ein Schutz der Daten gegen Zweckentfremdung, Aufklärungs- und Auskunftspflichten gegenüber dem Betroffenen, Löschungspflichten und eine unabhängige Kontrolle durch Datenschutzbeauftragte erforderlich [BVerfG 1983, S. 46].

Das Recht auf informationelle Selbstbestimmung umfaßt alle personenbezogenen Daten. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (§ 3 Abs. 1 BDSG). Durch die Verknüpfung mit anderen Daten kann auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; „belanglose“ Daten gibt daher nicht [BVerfG 1983, S. 45]. Zu den personenbezogenen Daten zählen auch Namen, Pseudonyme und andere Angaben, die der Identifizierung der Person dienen, ohne im übrigen etwas über sie auszusagen [Dammann 1992, § 3 Rdnr. 10].

Das Recht des Betroffenen, selbst über die Verwendung seiner Daten zu bestimmen, kann nur in den Fällen eingeschränkt werden, in denen dies im überwiegenden Allgemeininteresse erforderlich ist. Die Voraussetzungen und der Umfang der Beschränkungen müssen entsprechend dem Gebot der Normenklarheit für den Betroffen nachvollziehbar in einem Gesetz geregelt werden; der Grundsatz der Verhältnismäßigkeit muß beachtet werden [BVerfG 1983, S. 44].

2.1.1.2 Das Fernmeldegeheimnis

Im Bereich der Kommunikation wird das Recht auf informationelle Selbstbestimmung durch das Brief-, Post- und Fernmeldegeheimnis (Art. 10 GG) ergänzt.

Die Grundrechte des Art. 10 GG schützen die Vertraulichkeit individueller Kommunikation, sofern diese wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist [BVerfG 1992, S. 396] und deshalb dem Zugriff Dritter, insbesondere staatlicher Stellen, in besonderer Weise offensteht. Art. 10 GG gewährleistet die Verfügungsbefugnis über Informationen, die übermittelte Kommunikationsvorgänge betreffen, einschließlich der Befugnis, z. B. durch den Einsatz kryptographischer Verfahren Vorkehrungen gegen ungewollte Kenntnisnahme durch Dritte zu treffen [Hermes 1996, Rdnr. 13].

Das Postgeheimnis schützt die Vertraulichkeit der über die Post in der Ausübung öffentlicher Gewalt abgewickelten Kommunikationsvorgänge. Das Brief- und das Fernmeldegeheimnis knüpfen unabhängig vom Vermittler an das Kommunikationsmedium an. Das Briefgeheimnis schützt die Vertraulichkeit schriftlich fixierter individueller Mitteilungen; dem Fernmeldegeheimnis unterliegen alle körperlos übertragenen individuellen Mitteilungen [Hermes 1996, Krüger 1996].

Das Fernmeldegeheimnis gilt unabhängig davon, welche Übertragungsart genutzt wird, wer Betreiber der Vermittlungseinrichtungen ist und ob diese öffentlich oder nur für einen bestimmten Teilnehmerkreis zugänglich sind; auch auf die Art der übertragenen Daten kommt es nicht an [Hermes 1996, Rdnr. 33, 36]. Im Hinblick auf neue elektronische Übertragungsmöglichkeiten ist das Fernmeldegeheimnis dynamisch [Krüger 1996, Rdnr. 14]. Dem Schutz der Vertraulichkeit unterliegen neben dem Kommunikationsinhalt auch die Angaben über den Kommunikationsvorgang, insbesondere ob und wann zwischen welchen Personen Fernmeldeverkehr stattgefunden hat [BVerfG 1992, S. 396]. Geschützt ist nur die individuelle Kommunikation; angesichts der zunehmenden Vermischung von Individual- und Massenkommunikation genügt für den Schutz des Fernmeldegeheimnisses aber bereits die Möglichkeit, daß auf dem Übertragungsweg individuelle Kommunikationsvorgänge stattfinden [Hermes 1996, Rdnr. 35].

Das Fernmeldegeheimnis darf durch Gesetze eingeschränkt werden. Die Überwachung und Aufzeichnung des Fernmeldeverkehrs darf nach § 100a StPO zu Zwecken der Strafverfolgung und nach § 39a AWG zur Verhütung von Straftaten nach dem Außenwirtschafts- und Kriegswaffenkontrollgesetz angeordnet werden. Diese Maßnahmen kann, außer bei Gefahr im Verzug, nur ein Richter treffen. Darüberhinaus sind Eingriffe zu Zwecken des Staats- und Verfassungsschutzes zulässig. Bei der Einschränkung des Fernmeldegeheimnisses sind sind die Grundsätze der Normenklarheit und der Verhältnismäßigkeit zu berücksichtigen [Hermes 1996]. Dies gilt auch für Eingriffe, die aus betrieblichen Gründen oder zum Schutz anderer Teilnehmer vor Mißbrauch nötig sind [BVerfG 1992, S. 397 f.].

2.1.2 Das traditionelle Datenschutzkonzept

Die bisherigen Datenschutzgesetze sind vor dem Hintergrund der inzwischen weitgehend überholten Technologie der siebziger Jahre entstanden [Rat 1995]. Dem Leitbild der zentralen Datenverarbeitung gemäß orientiert sich ihr Datenschutzkonzept am Bestehen einer Datei mit personenbezogenen Daten, einer verantwortlichen datenverarbeitenden Stelle und einer Datenverarbeitungsanlage [Roßnagel 1997b]. Die Einrichtung einer neuen Datei mußte die zuständige Fachabteilung dabei jeweils bei der Datenverarbeitungszentrale beantragen; der Ablauf der Verarbeitungsprozesse war im voraus festgelegt [Nitsch 1995].

Den Konsequenzen dieser Datenverarbeitung für die informationelle Selbstbestimmung wurde ein rein normativ gestalteter Datenschutz entgegengesetzt [Roßnagel 1997b]: Für die Verarbeitung personenbezogener Daten besteht ein Verbot mit Erlaubnisvorbehalt für gesetzlich zugelassene oder mit dem Betroffenen vereinbarte Zwecke. Über die Dateien öffentlicher Stellen wird ein Register geführt; nichtöffentliche Stellen, die Daten zum Zweck der Übermittlung oder Auftragsverarbeitung speichern, sind meldepflichtig. Die Einhaltung der Datenschutzvorschriften wird von Datenschutzbeauftragten und einer Aufsichtsbehörde für den nichtöffentlichen Bereich überwacht.

2.1.3 Datenspuren

Datennetze werden zur Kommunikation, zum Zugriff auf Informationen und zum Bestellen von Waren genutzt. Mit der Zahl ihrer Anwendungen wächst auch die Zahl der Alltagstätigkeiten und -transaktionen, die elektronisch abgewickelt werden [Rexrodt 1997]. Dabei hinterläßt potentiell jede Aktion dauerhafte Spuren. Anders als beim Kauf gegen Bargeld läßt sich bei einem Netzdienst detailliert feststellen und dauerhaft speichern, wie lange jemand beispielsweise welchen Zeitungsartikel gelesen hat.

2.1.3.1 Zugriff auf WWW-Seiten

Auf unvoreingenommene Nutzer macht das WWW in der Regel den Eindruck, sie könnten dort unbeobachtet lesen und nach Informationen suchen.

Tatsächlich übertragen Browser wie Netscape Navigator (Netscape Communications Inc.) und Internet Explorer (Microsoft Corp.) bei einer Anfrage an einen WWW-Server nicht nur den URL der gewünschten Seite, sondern unter anderem auch die verwendete Browser- und Betriebssystemversion, eine Liste akzeptierter Datentypen und im `Referer`-Header den URL der Seite, von der der Nutzer bei der Benutzung eines Hypertext-Links gekommen ist. Standard-Server protokollieren bei jedem Zugriff das aufgerufene Objekt, den `Referer`, die Internet-Adresse des Abrufers, den verwendeten Browser sowie Datum und Uhrzeit [Damker 1997, Kubicek 1996].

Diese Daten ermöglichen die Analyse des Verhaltens und der Interessen des Abrufers. Über den Referer läßt sich verfolgen, wie sich der Nutzer durch das WWW-Angebot bewegt, mit welcher Such-Anfrage er auf einen Server gelangt ist oder welchen Namen eine private Datei hat, von der aus er den Server aufruft.

Der Internet Explorer 4.0 überträgt an Betreiber von Push-Kanälen auf Anforderung eine Datei, aus der sowohl Online-Zugriffe als auch Zugriffe auf beim Nutzer gespeicherte Seiten des Angebots hervorgehen, sofern der Nutzer diese Funktion nicht deaktiviert hat. Übermittelt werden auch Zeitpunkt und Dauer des Zugriffs. Die `LOG-TARGET`-Anweisung spezifiziert, an welche Adresse der Browser die Datei senden soll [Ellerman 1997].

Sogenannte *Cookies* [Kristol 1997] ermöglichen es, im Übertragungsprotokoll HTTP für eine Sitzung oder auch über mehrere Sitzungen hinweg Zustandsinformationen zu übertragen. Damit soll die Implementation beispielsweise von personalisierten Einstiegsseiten und von Warenkorb-Funktionen erleichtert werden. Am häufigsten werden Cookies aber dazu verwendet, die Zugriffe von Nutzern auf verschiedene WWW-Server zu verketten, um ihnen gezielt Werbung präsentieren zu können [Damker 1997]. Die Firma, von der die Werbeeinblendungen kommen, erhält im `Referer` Informationen über die Seite, die er aufgerufen hat und kann den Nutzer über einen Cookie identifizieren. Über Nutzerprofile kann so die jeweils effizienteste Werbeeinblendung ausgewählt werden.

Oft ist auch die Identität des einzelnen Nutzers feststellbar. Über den `finger`-Dienst [Zimmerman 1991] lassen sich Namen, E-Mail-Adressen und weitere Informationen über die auf dem Rechner eingeloggten Personen feststellen. Das für Audit-Zwecke gedachte Identifikations-Protokoll [Johns 1993] übermittelt eine den Eigentümer einer bestimmten TCP-Verbindung identifizierende Zeichenkette, üblicherweise den Login-Namen. Bei T-Online, dem größten Internet-Zugangsanbieter in Deutschland, ist dies in der Regel die Telefonnummer des Kunden[1].

Diese Informationen kann der Server-Betreiber ohne Wissen und Kontrollmöglichkeit des Nutzers erlangen.

[1] Auf Antrag wird auch eine andere Nummer zugeteilt. Wenn der Nutzer jedoch einmal einen Text in einer Newsgroup oder einer im WWW archivierten Mailing-Liste veröffentlicht hat, ist sein Name trotzdem über eine Suchmaschine feststellbar.

WWW-Browser bieten die Möglichkeit, aus dem Netz geladene Programme auszuführen. Plug-Ins sind Software-Module, die den Funktionsumfang eines Browsers zum Beispiel für Multimedia-Anwendungen erweitern; ActiveX-Controls sind Programmbibliotheken, die der Internet Explorer von WWW-Servern laden und ausführen kann. Java-Applets werden ebenso wie ActiveX-Controls benutzt, um die Darstellung von Inhalten durch Programme zu ergänzen; sie werden aber innerhalb des Browsers ausgeführt.

Plug-Ins und ActiveX-Controls haben alle Zugriffsrechte des Nutzers auf System-Ressourcen, sie können also auf seine Daten zugreifen und sie unbemerkt übertragen und sogar verändern oder zerstören. Der Internet Explorer kann die Herkunft und Integrität von Controls anhand einer digitalen Signatur prüfen. Zertifiziert wird aber nur ihre Herkunft, nicht die Funktionalität. Trotz der Signatur besteht also die Gefahr, daß ein Programm absichtlich oder durch einen Fehler die Vertraulichkeit der Daten des Anwenders gefährdet [Koke 1997].

Java-Applets werden in einem plattformunabhängigen Bytecode übertragen und innerhalb einer virtuellen Maschine ausgeführt. Verletzungen der Zugriffssemantik der Sprache und die Ausführung schädlicher Funktionen sollen erkannt und abgefangen werden. Es wurden jedoch verschiedene Möglichkeiten entdeckt, das Sicherheitssystem aufgrund von Implementationsfehlern und Schwächen im Entwurf zu umgehen und damit Zugriff auf Daten des Nutzers zu erhalten. Es ist kaum möglich, die Sicherheit eines so komplexen, vom Entwurf her nicht formal spezifizierten Systems zu beweisen [Dean 1996].

Zudem wurden verschiedene Fehler in den Browsern selbst bekannt, durch die nicht vorgesehene Zugriffe auf Daten des Nutzers möglich werden [Martienssen 1997].

2.1.3.2 Electronic Mail

Am Transport von E-Mail sind häufig verschiedene Netzknoten beteiligt, auf denen die Nachrichten zwischengespeichert werden. Meist werden die Nachrichten auf einem Rechner des Netzbetreibers gespeichert, bis der Empfänger sie abruft. Die Administratoren aller beteiligten Systeme können diese Nachrichten ohne weiteres mitlesen. Wenn eine Nachricht nicht zugestellt werden kann, wird oft eine Kopie an den Administrator des Absendersystems geschickt [Eklund 1996].

Mit Hilfe von Logfiles der beteiligten Mail-Systeme können Kommunikationsbeziehungen überwacht werden. Das häufig eingesetzte System `sendmail` speichert standardmäßig die Adressen von Absender und Empfänger sowie Datum und Uhrzeit jeder Nachricht. Die Protokolle werden meist einige Monate aufbewahrt, können aber auch länger archiviert werden. Kommunikationsprofile können so mit geringem Aufwand erstellt werden, auch wenn die eigentlichen Nachrichten nicht mehr gespeichert sind [Schallbruch 1995].

2.1.3.3 Usenet News

In öffentlichen Foren wie den Usenet-Newsgroups werden alle erdenklichen Themen diskutiert, darunter auch sensible Themen wie Selbsthilfe bei persönlichen Problemen.

Beiträge in Newsgroups haben oft einen spontanen Charakter; sie gleichen eher einer Äußerung in einem persönlichen Gespräch oder einer Stammtischrunde als einer Veröffentlichung [Mayer 1997]. Allerdings sind diese Beiträge weltweit verfügbar. Unternehmen wie DejaNews bieten die Möglichkeit, Newsgroups nach Autoren und Stichwörtern zu durchsuchen. DejaNews erstellt auch Autoren-Profile, in denen sämtliche Usenet-Artikel eines Autors aufgelistet sind. Das Unternehmen beabsichtigt, langfristig alle seit 1979 veröffentlichten Usenet-Artikel zugänglich zu machen [Ulfelder 1996].

2.1.3.4 Digitale Zahlungssysteme

Mit dem Wachstum des elektronischen Handels gewinnt die Frage an Bedeutung, wie der Zahlungsverkehr abgewickelt werden soll. Es geht dabei nicht nur um Waren, die jetzt schon per Kreditkarte bezahlt werden, sondern vor allem um geringfügige Beträge für den Abruf einzelner Informations- und Unterhaltungsangebote. Durch die Informationstechnik werden auch Zahlungen im Pfennigbereich *(„Micropayments“)* rentabel. Würde dabei jeder Abruf einer Evidenzzentrale[2] gemeldet, entstünde dort ein so detailliertes Persönlichkeitsbild, daß viele Nutzer Informationen nicht mehr unbefangen anfordern würden [BfD 1997].

2.1.3.5 Vermittlungs- und Transportschicht

Im Unterschied zu traditionellen Fernmeldenetzen wird das Internet nicht von einer einzelnen Behörde betrieben, sondern von einer Vielzahl privater Netzbetreiber. Ihnen gemeinsam ist die Datenübertragung nach dem verbindungslosen Internet Protocol [Postel 1981], auf dem das verbindungsorientierte Transmission Control Protocol [Postel 1981b] aufsetzt. Die Übertragung erfolgt bisher in der Regel unverschlüsselt und kann daher an allen an der Übertragung beteiligten Stellen abgehört und automatisiert nach interessanten Daten durchsucht werden. Es wird vermutet, daß einige der wichtigsten Internet-Knoten von der amerikanischen National Security Agency abgehört werden [Dillon 1996].

2.1.4 Neue Möglichkeiten der Auswertung

Neben der Beobachtbarkeit von Aktionen des Nutzers wirken sich auch neue Möglichkeiten zur Datenauswertung auf den Datenschutz aus.

Über das Internet sind Informationen verschiedenster Anbieter zugänglich. Die Daten können unbegrenzt lange gespeichert werden; aufgrund der Preisentwicklung ist die Verfügbarkeit von Speicherplatz dabei nicht mehr problematisch. WWW-Seiten und Newsgroups werden von Suchmaschinen automatisch indiziert. Diese Suchmaschinen erlauben es Nutzern, Millionen von Dokumenten nach Stichworten zu durchsuchen. Intelligente Agenten können auch auf Informationsdienste wie Datenbanken

[2] Transaktionsdaten für Zahlungen mit der *GeldKarte* der deutschen Banken werden an eine Evidenzzentrale weitergeleitet, die die Daten kontrolliert und ein Saldo für die Karte führt.

automatisiert zugreifen und gewünschte Informationen liefern [Etzioni 1996]. Mit Data-Mining-Techniken können neue Zusammenhänge in großen Datenmengen entdeckt werden [Schweighofer 1997].

So entsteht ein „Dossier-Effekt“ [Goldberg 1997]: Es wird möglich, mit einer einfachen Anfrage über eine Person ein umfassendes Profil mit Daten aus verschiedenen Quellen wie Newsgroups, Zeitungen, Zeitschriften, kommerziellen Datenbanken und amtlichen Dokumenten zu erhalten.

2.1.5 Mangelnde Kontrollmöglichkeiten

Im Internet liegen personenbezogene Daten nicht mehr in klar festgelegten Dateien vor. Auch ihre Verarbeitung erfolgt nicht mehr in einer Datenverarbeitungsanlage, sondern im Netz verteilt. Daten werden von vielen Beteiligten verarbeitet, ohne daß es einen verantwortlichen Betreiber gibt [Roßnagel 1997b].

Der Datenschutz läßt sich vor allem dann wirkungsvoll kontrollieren, wenn die Verarbeitung personenbezogener Daten bei wenigen Stellen konzentriert ist. Wenn die fortgeschrittene Vernetzung die Ablösung großer zentraler Datenbanken durch Netze kleiner verknüpfter Datenbanken ermöglicht, wird die Regulierung zunehmend schwierig [Froomkin 1996].

Da im Internet an jedem Übertragungsvorgang diverse private Netzbetreiber beteiligt sind, die sich zudem in Staaten mit sehr unterschiedlichem Datenschutzrecht befinden, ist die Einhaltung des Datenschutzes kaum noch zu überwachen.

2.1.6 Auswirkungen der Globalisierung

Die internationale Vernetzung könnte die Durchsetzbarkeit von Datenschutzgesetzen völlig aushebeln. Zwar ist die Übermittlung personenbezogener Daten in das Ausland nach Art. 25 der EG-Datenschutzrichtlinie an ein angemessenes Datenschutzniveau geknüpft, aber in globalen Netzen ist diese Forderung kaum zu kontrollieren. Theoretisch müßte jeder europäische Inhaltsanbieter überprüfen, ob der Abrufer die jeweilige Information erhalten darf [Schweighofer 1997]; solange ein Land aber an das Internet angeschlossen ist, sind Exportverbote für Informationen wegen des internationalen Charakters des Netzes nicht durchsetzbar [Froomkin 1996, Roßnagel 1997b].

Inhaltsanbieter können personenbezogene Daten in Ländern ohne hinreichende Datenschutzgesetzgebung anbieten [Budapest 1996]. Selbst internationale Vereinbarungen könnte ein einzelner Staat analog zu Steueroasen in der Form einer „Daten-Oase“ unterlaufen [Froomkin 1996].

Das bisherige Datenschutzkonzept kann die verfassungsmäßigen Anforderungen daher nicht mehr erfüllen. Angesichts der dennoch wachsenden Gefahren für den Datenschutz und die Vertraulichkeit der Kommunikation muß der Staat vom Teilnehmer selbst kontrollierbaren technischen Datenschutz fördern [Roßnagel 1997].

2.1.7 Datenschutz gewährleistende Technik in Kommunikationsnetzen

Nach Ansicht der Bundesregierung kann die informationelle Selbstbestimmung in globalen Netzen nur durch größtmögliche Anonymität des Nutzers gewährleistet werden [Bundestag 1997]. Mit dem TDDSG und dem MDStV wird der Datenschutz bei der Nutzung von Informations- und Kommunikationsdiensten geregelt. Für Diensteanbieter gilt das Gebot der Datenvermeidung (§ 3 Abs. 4 TDDSG): Angebote sollen an dem Ziel ausgerichtet werden, keine oder jedenfalls so wenige personenbezogene Daten wie möglich zu erheben und zu verarbeiten [Bundestag 1997]. Konkretisiert wird dieses Ziel durch die Pflicht, Nutzung und Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies – abhängig von den technischen Möglichkeiten und von der wirtschaftlichen Leistungsfähigkeit des Anbieters – möglich und zumutbar ist (§ 4 TDDSG).

Anonymität ist das Fehlen von Personenbezug. Faktische Anonymität bedeutet, daß die Zuordnung des Nutzungsvorgangs zu einer Person nur mit unverhältnismäßig großem Aufwand möglich ist; dies reicht für das Erfordernis der Anonymität aus [Bundestag 1997]. Ein Pseudonym ist ein Name oder eine Kurzbezeichnung, die die Identität des Nutzers nicht aus sich heraus erkennen läßt (vgl. Abschnitt 3.4).

Ein bestimmtes Verfahren zur Realisierung von Anonymität und Pseudonymität wird nicht vorgeschrieben. Im Rahmen der gesetzlichen Vorgaben sollen verschiedene technische Verfahren im Wettbewerb untereinander erprobt werden können.

2.2 Zulässigkeit kryptographischer Verfahren

2.2.1 Die Kryptokontroverse

Kryptographische Verfahren, die die Vertraulichkeit übertragener Daten sichern, bedrohen gleichzeitig die Möglichkeit von Strafverfolgungsbehörden, die Kommunikation von Kriminellen abzuhören. Daher wird diskutiert, Verfahren zu verbieten, die die zuständigen Behörden nicht entschlüsseln können.

Innenminister Kanther sprach sich im März 1997 auf dem BSI-Kongreß dafür aus, die Abhörmöglichkeiten durch eine Schlüsselhinterlegungspflicht zu gewährleisten [KES 1997]. In der Enquete-Kommission „Zukunft der Medien“ des Bundestages warnten die angehörten Experten, ein Verbot oder strenge Auflagen für Verschlüsselungstechniken würden mehr Schaden als Nutzen stiften [WiB 1997]. Innerhalb der Bundesregierung war der Vorschlag Kanthers umstritten; Wirtschaftsverbände und Datenschützer sprachen sich dagegen aus.

Mit dem Signaturgesetz wurde die Grundlage für eine staatlich anerkannte Infrastruktur für digitale Signaturen auf der Basis kryptographischer Verfahren geschaffen; über den Einsatz kryptographischer Verfahren zur Verschlüsselung wurde dabei aber keine Aussage getroffen. Das Innenministerium setzt nun zunächst auf eine freiwillige Schlüsselhinterlegung [Bizer 1997].

Die US-Regierung versuchte 1991, die Abhörbarkeit verschlüsselter Kommunikation durch die freiwillige Einführung des *Escrowed Encryption Standard* und des darauf beruhenden Clipper-Chips zu sichern, der eine Entschlüsselungsmöglichkeit für Strafverfolgungsbehörden bereitstellt. Dieser Standard konnte sich jedoch nicht durchsetzen. Verschlüsselungstechnologie unterliegt in den USA der Exportkontrolle; zulässig ist nur der Export von Verfahren, die mit geringem Aufwand entschlüsselt werden können oder eine Entschlüsselungsmöglichkeit für US-Behörden beinhalten. Diese Exportkontrolle stößt auf die Kritik vieler Softwarehersteller, die damit auf dem internationalen Markt Wettbewerbsnachteile hinnehmen müssen. Ihre Zulässigkeit ist Gegenstand mehrerer Gerichtsverfahren. 1997 haben Strafverfolgungsbehörden die Beschränkung kryptographischer Verfahren auch innerhalb der USA vorgeschlagen.

2.2.2 Durchsetzbarkeit gesetzlicher Regelungen

Um den Zugriff der zuständigen Behörden auf die Kommunikation in Netzen sicherzustellen, kommt zum einen ein vollständiges Verbot aller Verschlüsselungsverfahren, zum anderen ein Verbot unter dem Vorbehalt einer Zulassung im Einzelfall für Verfahren mit Entschlüsselungsmöglichkeit der Sicherheitsbehörden in Frage.

Ein Eingriff in das Fernmeldegeheimnis ist nur zulässig, wenn er verhältnismäßig ist. Bei Beschränkungen von Verschlüsselungsverfahren ist diese Voraussetzung nur dann erfüllt, wenn sie geeignet sind, die Interessen der Inneren Sicherheit effektiv zu wahren [Bizer 1995].

Ein Verbot würde die Rechte aller Teilnehmer einschränken, nur um dem Staat das Abhören in wenigen Einzelfällen zu ermöglichen. Dadurch würde die Erbringung wichtiger Dienste, besonders für die kommerzielle Nutzung von Kommunikationsnetzen, verhindert; auch Kriminelle könnten Daten abhören und verfälschen.

Die für die staatliche Überwachung interessanten Personenkreise hätten trotzdem die Möglichkeit, unbeobachtet zu kommunizieren: Sofern überhaupt die Übertragung von Information möglich ist, können Sender und Empfänger immer auch eine geheime Zusatzbedeutung des scheinbaren Klartextes vereinbaren. Es ist möglich, in datenintensiven Anwendungen wie Audio- oder Video-Kommunikation geheime Nachrichten zu verbergen (Steganographie) [Huhn 1997].

Auch staatlich genehmigte Verschlüsselungs- und Signatursysteme können Kriminelle trotz der vorgesehenen Entschlüsselungsmöglichkeit für ihre Zwecke ausnutzen.

Eine Sicherungsinfrastruktur für Signatursysteme, wie sie im Rahmen des SigG bereitgestellt wird, kann zum sicheren Austausch von Schlüsseln für ein Verschlüsselungssystem verwendet werden. Es läßt sich nicht verhindern, daß Kriminelle selbst Schlüssel generieren und mit Hilfe der öffentlichen Signatur-Infrastruktur zertifizieren.

Ein staatlich genehmigtes Verschlüsselungsverfahren kann für die unbemerkte Verwendung nicht genehmigter asymmetrischer Verschlüsselungsverfahren ausgenutzt werden. Dabei werden zunächst die selbstgenerierten, nicht hinterlegten öffentlichen Schlüssel mit dem genehmigten Verfahren verschlüsselt und dem Kommunikationspartner mitgeteilt. Die Nachrichten selbst verschlüsselt der Kommunikationspartner zunächst mit dem selbstgenerierten Schlüssel, und dann ein zweites Mal mit dem hinterlegten. Die resultierende Kommunikation wirkt nach außen hin wie vorschriftsmäßig entschlüsselbare. Erst wenn eine Entschlüsselung angeordnet wird, stellt die zuständige Behörde fest, daß die Nachricht nicht lesbar ist [Hamm 1997].

Ein Verbot würde gerade in den Fällen, in denen der Zugriff durch Strafverfolgungsbehörden nötig wird, keine ausreichende Abschreckungswirkung haben. In diesen Fällen wird die Strafe für unerlaubte Verschlüsselung meist erheblich niedriger sein als die für die damit getarnten schweren Straftaten [Bizer 1995].

Für gesetzestreue Anwender bringt die Hinterlegung der Kommunikationsschlüssel bei einer externen Stelle jedoch zusätzliche Kosten und neue Risiken mit sich. Es entsteht ein zusätzlicher Angriffspunkt, an dem eine große Menge höchst sensibler Daten langfristig gespeichert wird. Ein zuverlässiger Schutz ist auch für sämtliche Stellen (z. B. Staatsanwaltschaften) erforderlich, von denen aus diese Daten automatisiert abgerufen werden können. Unabhängig von den konkreten Sicherungsmaßnahmen besteht die Gefahr, daß durch Bestechung oder Erpressung Daten kompromittiert werden. Durch zusätzliche Entschlüsselungsmöglichkeiten erhöht sich die Komplexität des kryptographischen Systems erheblich. Damit werden Entwurf und Analyse des Systems erschwert und die Wahrscheinlichkeit gravierender Fehler steigt an. Die Sicherung der hinterlegten Schlüssel und eine Infrastruktur, die die Schlüssel allen Bedarfsträgern kurzfristig zur Verfügung stellen kann, wären sehr kostenaufwendig [Abelson 1997].

Da Beschränkungen kryptographischer Verfahren gerade von Kriminellen leicht umgangen werden können, aber die Rechte legitimer Nutzer einschränken, sind sie für ihre Zwecke untauglich und daher nicht verhältnismäßig [Bizer 1995]. Ihre verfassungsrechtliche Zulässigkeit ist somit zweifelhaft.

2.3 Anonymität und ihre Grenzen

2.3.1 Anonymer Zugriff auf Informationen

Die Anonymität wirft über den Datenschutz hinaus rechtliche Fragen auf.

Weitgehend unproblematisch ist der anonyme Lesezugriff auf Informationsangebote. Allerdings besteht dabei die Gefahr, daß der Schutz der Anonymität von Angreifern ausgenutzt wird, um in ein System einzudringen [Goldberg 1997]. Sofern solche Angriffe nicht vom Anonymisierungsdienst entdeckt und verhindert werden können, führt das dazu, daß ein Angreifer nicht mehr im Nachhinein zur Rechenschaft gezogen werden kann. Diensteanbieter müssen somit verstärkten Wert darauf legen, daß ihr System von vornherein sicher gestaltet ist. Derartige Sicherheitsmaßnahmen sind aber schon wegen der durch die Internationalität des Netzes erschwerten Strafverfolgung erforderlich [NIST 1996].

2.3.2 Anonyme Äußerungen

Die Gefahr der Erstellung von Persönlichkeitsprofilen durch die Auswertung der Kommunikation beispielsweise in Usenet-Newsgroups (siehe Abschnitt 2.1.3.3) läßt sich durch die Verwendung zurückverfolgbarer Pseudonyme begrenzen.

Inwieweit darüberhinaus auch anonyme Äußerungen zulässig sind, wird schon seit langem diskutiert. Gründe für Anonymität können unter anderem die Diskussion sensibler persönlicher Angelegenheiten, die Suche nach Information, Redefreiheit in intoleranten Umgebungen sowie die Teilnahmen an Abstimmungen oder Umfragen sein [Gülcü 1996].

Wer bei medizinischen Problemen, als Opfer eines Verbrechens oder als Sektenaussteiger Hilfe sucht oder sich mit anderen Betroffenen austauschen möchte, würde ein Angebot möglicherweise nicht nutzen, wenn die Gefahr besteht, daß Menschen aus seinem persönlichen Umfeld davon erfahren. Daher ist oft entscheidend, daß die Identität des Nutzers geheim bleibt.

Der Nutzen der Anonymität ist aber nicht auf therapeutische Zwecke beschränkt. Wer sich beispielsweise über Möglichkeiten eines Stellenwechsels informiert, möchte häufig nicht, daß der gegenwärtige Arbeitgeber davon erfährt [Gülcü 1996, Hannaford 1996]. Bürger möchten oft Auskünfte bei Behörden einholen, ohne daß die Anfrage in einer Akte vermerkt wird. Firmen möchten z. B. Patentrecherchen durchführen können, ohne anderen Rückschlüsse auf ihre Forschungs- und Entwicklungsprojekte zu ermöglichen [Pfitzmann 1990]. Es kommt auch vor, daß jemand – etwa im Beruf – Hilfe bei einem Problem benötigt, obwohl von ihm erwartet wird, daß er die Lösung kennt [Detweiler 1993]. Für Prominente ist die Möglichkeit nützlich, inkognito an Diskussionen teilzunehmen [Seltzer 1995].

Von besonderem Nutzen ist Anonymität für die Redefreiheit in intoleranten Umgebungen. In autoritären und repressiven Staaten spielt die anonyme Nutzung des Internet eine bedeutende Rolle für die Kommunikation verfolgter Personen untereinander und mit dem Rest der Welt [EU-Parl. 1997]. Auch in der freien Welt kann die Äußerung unpopulärer Ansichten oder die Kritik an intoleranten oder fanatischen Gruppen gefährliche Folgen nach sich ziehen [Gülcü 1996]. Besonders gilt das für Strafanzeigen, die in manchen Fällen aus Furcht vor Rache nur gestellt werden, wenn der Betreffende sich sicher ist, daß seine Identität nicht bekannt wird. Ähnliches gilt für Firmen- oder Behördenangehörige, die von Repressionen bedroht sind, wenn sie Mißstände in ihrer Organisation öffentlich machen. Anonymität kann aber auch aus harmloseren Gründen berechtigt sein, zum Beispiel um unausgereifte Ideen erst einmal zu erproben, bevor man den eigenen Ruf damit aufs Spiel setzt [Engel 1996].

Schließlich ist auch das Wahlgeheimnis als eines der Grundprinzipien der Demokratie auf Anonymität angewiesen.

2.3.3 Gefahr des Mißbrauchs

Anonymität kann auch die Versendung illegalen Materials erleichtern, indem die Identifizierung der Täter erschwert oder sogar unmöglich wird [EU-Komm. 1996].

Über den finnischen „Anon-Server" `anon.penet.fi` wurden urheberrechtswidrig Texte und Software sowie pornographische Bilder verschickt, bis der Betreiber diese illegale Verbreitung durch eine Größenbegrenzung für die übertragenen Dateien verhindern konnte [Quittner 1995].

Auch der Verrat von Firmengeheimnissen wird durch Anonymität erleichtert. Beispielsweise wurde der Verschlüsselungsalgorithmus RC4 der Firma RSA Data Security im September 1994 anonym in einer Mailing-Liste veröffentlicht. Daraufhin wurde er weltweit verbreitet und in der Folge auch in Büchern veröffentlicht.

Es wird auch befürchtet, daß Anonymisierungsdienste von kriminellen Organisationen zur Kommunikation benutzt werden können [Strassmann 1996]; allerdings gibt es wenig dokumentierte Fälle [Hannaford 1996].

Bei anonymen Zahlungsmitteln besteht zudem die Gefahr der Geldwäsche. Im Gegensatz zu Bargeld kann digitales Geld auch in großen Mengen über Grenzen hinweg transportiert werden. Solange allerdings alle Zahlungen über eine Bank abgewickelt werden müssen und nur der Bezahler, aber nicht der Bezahlte anonym ist, wird Geldwäsche durch digitale Zahlungsmittel nicht wesentlich erleichtert [Froomkin 1996].

Anonyme Beschimpfungen sind ein recht häufiges Problem. Auch Belästigung durch unerwünschte Werbung findet oft im Schutz der Anonymität statt. Aufgrund der im Internet kaum begrenzten Verbreitungsmöglichkeiten ist üble Nachrede besonders bedrohlich, wenngleich anonyme Nachrichten i. a. nicht so glaubwürdig sind wie namentlich gekennzeichnete [Froomkin 1996].

Der Umfang des Mißbrauchs ist jedoch verhältnismäßig gering. Der Server `anon.penet.fi` leitete zwischen 1993 und 1996 täglich bis zu 10 000 E-Mail-Nachrichten und Usenet-Artikel pseudonymisiert weiter. Nur zweimal wurde polizeilich die Offenlegung von Pseudonymen verlangt, in beiden Fällen auf Veranlassung von Scientology, die die Adressen von Kritikern der Organisation erfahren wollte [Helmers 1997].

2.3.4 Anonymität in traditionellen Medien

2.3.4.1 Presserecht

Die Auseinandersetzung um die Anonymität ist so alt wie der Buchdruck. Im 16. Jahrhundert wurden die Impressumpflicht und die Folterung von Besitzern anonymer Schriften zur Feststellung des Verfassers eingeführt, da Mißstände der Zeit in anonymen Flugschriften öffentlich kritisiert wurden [Löffler 1994]. Im demokratischen Rechtsstaat besteht für die Presse einerseits eine Impressumpflicht, andererseits ein Recht auf publizistische Anonymität.

Die Impressumpflicht ist im besonderen Einfluß und damit der Gefährlichkeit der Presse begründet. Die Angabe von Namen und Anschrift des Druckers und des Verlegers soll es ermöglichen, die für den Inhalt eines Druckwerks Verantwortlichen jederzeit haftbar zu machen. Für die besonders einflußreiche periodische Presse besteht die

Pflicht, einen verantwortlichen Redakteur zu benennen, der die Druckschrift von strafbarem Inhalt freihalten muß und bei Verstößen persönlich haftet. „Harmlose“ Druckschriften, die ausschließlich familiären, gewerblichen oder ähnlichen Zwecken dienen, sind vom Impressumzwang freigestellt [Löffler 1983].

Der Verfasser muß nur aufgeführt werden, wenn er selbst als Verleger tätig ist. Ansonsten darf er anonym bleiben oder sich hinter einem Pseudonym verbergen. Das publizistische Zeugnisverweigerungsrecht erlaubt es der Presse, die Anonymität von Verfassern und Informanten zu schützen, selbst wenn dies der Verfolgung einer schweren Straftat entgegensteht [Löffler 1994]. In diesen Schutz sind auch die Autoren anonym veröffentlichter Leserbriefe einbezogen.

Das Presserecht gilt nur für körperlich vervielfältigte Werke. Für den ebenfalls einflußreichen Rundfunk existiert eine entsprechende Regelung der Verantwortlichkeit.

Bei Briefen ist das Recht auf Anonymität nicht eingeschränkt.

2.3.4.2 Telefonie

Wenn in einem Telefonnetz die Möglichkeit besteht, dem angerufenen Anschluß die Rufnummer des Anrufers zu übermitteln, muß der Telefonkunde die Möglichkeit haben, die Übermittlung dauerhaft (§ 9 TDSV) und nach Art. 8 der ab Oktober 1998 umzusetzenden ISDN-Richtlinie der EU auch fallweise zu unterdrücken. Darüberhinaus besteht die Möglichkeit, in Telefonzellen anonym zu telefonieren.

Bei bedrohenden oder belästigenden Anrufen werden die Anschlüsse, von denen die Anrufe ausgehen, auf Antrag mitgeteilt (§ 8 TDSV, Art. 9 ISDN-Richtlinie). Diese Einschränkung des Fernmeldegeheimnisses ist zur Abwehr derartiger Angriffe und zur Geltendmachung zivilrechtlicher Unterlassungs- und Schadensersatzansprüche erforderlich [BVerfG 1992].

Die ISDN-Richtlinie (Art. 8) sieht auch die Möglichkeit vor, eingehende Anrufe ohne Rufnummernübermittlung automatisch abzuweisen.

2.3.5 Anonymität im Internet

Wie bei den traditionellen Medien, so gibt es auch im Internet Dienste, bei denen Anonymität sinnvoll ist und andere, bei denen Identifikation erforderlich ist [LAB 1997].

Regelungen hierüber treffen der Mediendienste-Staatsvertrag und das Informations- und Kommunikationsdienstegesetz.

2.3.5.1 Mediendienste

Mediendienste sind Verteil- und Abrufdienste, bei denen die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht [Bundestag 1997].

Für diese Dienste ist, auch bei privaten Anbietern, nach § 6 MDStV eine Anbieterkennzeichnung mit Name und Anschrift vorgeschrieben. Dies dient dem Verbraucherschutz, öffentlichen Ordnungsinteressen, der Offenheit des Meinungsbildungsprozesses und der Rechtsverfolgung im Streitfall [Bundesrat 1997]. Bei journalistisch-redaktionell gestalteten Angeboten mit periodischer Verbreitung ist wie bei der periodischen Presse ein Verantwortlicher zu bestellen.

2.3.5.2 Teledienste

Bei Telediensten ist die Anbieterkennzeichnung nur für geschäftsmäßige Angebote vorgeschrieben (§ 6 TDG), nicht für private Gelegenheitsangebote.

Anbieter ist nicht, wer beispielsweise per E-Mail, Chat oder in einer Newsgroup Äußerungen mit kurzfristigem spontanen Charakter macht [Mayer 1997]; bei diesen Fällen handelt es sich um die Nutzung eines Teledienstes bzw. Mediendienstes. Die Nutzung aller Teledienste muß in anonymer oder pseudonymer Form ermöglicht werden [Bundestag 1997].

2.3.6 Aufdeckung von Pseudonymen

Das Signaturgesetz regelt eine Infrastruktur für den digitaler Signaturen im Rechtsverkehr, beispielsweise zur Bestellung von Waren. Um die Zuordnung einer Person zu einem Persönlichkeitsprofil z. B. bezüglich des Kaufverhaltens zu erschweren, werden Signaturschlüssel-Zertifikate auch auf Pseudonyme ausgestellt (§ 5 Abs. 3 SigG). Wenn der Schlüsselinhaber eine Bestellung oder Buchung tätigt, dann aber die eingegangenen Verpflichtungen nicht erfüllt, ist eine unbürokratische Aufdeckung des Pseudonyms erforderlich. Die Daten über die Identität des Signaturschlüssel-Inhabers müssen daher auf Ersuchen an die zuständigen Stellen übermittelt werden, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Gefahrenabwehr oder zur Erfüllung der Aufgaben der Sicherheitsdienste erforderlich ist (§ 12 Abs. 2 SigG). Der Inhaber ist davon zu unterrichten.

Für Pseudonyme, die nicht im Rahmen des Signaturgesetzes eingesetzt werden, gibt es keine solche Vorschrift.

Wird die Anonymität zur Begehung von Straftaten ausgenutzt, können die Ermittlungsmöglichkeiten der Strafprozeßordnung ausgeschöpft werden [Bundestag 1997]. In staatsanwaltschaftlichen Ermittlungsverfahren sind Betreiber von Anonymisierungsdiensten gemäß § 161a StPO verpflichtet, als Zeugen auszusagen. Nach § 103 StPO ist auch eine Durchsuchung bei Nichtverdächtigen und, wenn keine weniger einschneidenden Mittel zur Verfügung stehen, die Beschlagnahme von Datenträgern möglich [Laufhütte 1987]. Ob und inwieweit private Unternehmen schon bei Ermittlungen im Vorfeld der Strafverfolgung zu Auskünften über Bestandsdaten verpflichtet werden sollen, ist noch nicht geklärt [Engel-Flechsig 1997].

Die EU-Kommission und das Europäische Parlament fordern, daß im Internet alle anonymen Nachrichten zum Absender zurückverfolgbar sein müssen

[EU-Komm. 1996, EU-Parl. 1997]. Ob derartige Maßnahmen rechtlich zulässig sind, die grundsätzlich alle Spuren registrieren, um bei Gesetzesverstößen die Aufspürbarkeit des Täters zu gewährleisten, ist aber zweifelhaft [Simitis 1997].

Effektiv durchsetzbar ist diese Forderung nur, wenn sie weltweit umgesetzt wird. Daher muß auch berücksichtigt werden, wie andere Länder mit dem Problem der Anonymität umgehen.

2.3.7 Recht auf Anonymität in den USA

1960 hat der Supreme Court die Impressumpflicht für Flugblätter für verfassungswidrig erklärt, weil sie zu Furcht vor Repressalien führen und damit von friedlicher Diskussion wichtiger öffentlicher Angelegenheiten abschrecken könne. Anonyme Pamphlete, Broschüren und Bücher hätten für den Fortschritt der Menschheit eine wichtige Rolle gespielt. Immer wieder hätten im Laufe der Geschichte verfolgte Gruppen und Glaubensgemeinschaften unterdrückerische Praktiken nicht anders als anonym kritisieren können; sogar die Aufrufe für die Annahme der amerikanischen Verfassung seien unter fiktiven Namen veröffentlicht worden [USSC 1960].

Auch 1995 hat das Gericht das Recht eines Autors, anonym zu bleiben, wieder betont. Ob Verbote für – insbesondere unpolitische – anonyme Äußerungen dennoch unter bestimmten Bedingungen verfassungsgemäß sein könnten, ist unklar [Froomkin 1996]. Ein Gesetz des Bundesstaates Georgia, das anonyme Nutzung des Internet möglicherweise verboten hätte, wurde 1997 als verfassungswidrig außer Kraft gesetzt [Geogia 1997].

2.3.8 Anforderungen an Anonymisierungsdienste

Diensteanbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang vermitteln, nicht verantwortlich (§ 5 Abs. 3 TDG). Zu Sperrungen nach den allgemeinen Gesetzen sind sie verpflichtet, wenn sie unter Wahrung des Fernmeldegeheimnisses von den Inhalten erfahren haben und eine Sperrung technisch möglich und zumutbar ist (§ 5 Abs. 4 TDG). Neben gesetzlichen Sperrpflichten kann auch ein Verhaltenskodex für Betreiber von Anonymisierungsdiensten sinnvoll sein [WP 1996].

Folgende Anforderungen an den Betrieb eines Anonymisierungsdienstes wurden vorgeschlagen:

- Jeder Empfänger muß die Möglichkeit haben, anonyme E-Mail abzulehnen; entsprechendes wäre auch für Newsgroups denkbar [WP 1996].
- Anonyme Nachrichten sollten offen als solche gekennzeichnet sein, um schädliche Effekte der Anonymität zu begrenzen [Lee 1996].
- Wenn die Möglichkeit besteht, Pseudonyme aufzudecken oder anonyme Nachrichten zurückzuverfolgen, muß der Nutzer die Bedingungen dafür im voraus kennen [Rossum 1995].

2.3.9 Fazit

Die anonyme Nutzbarkeit von Netzdiensten ist wichtig für den Datenschutz. Bei einigen Diensten besteht jedoch die Gefahr des Mißbrauchs. Die Belästigung durch anonyme E-Mail kann durch Sperren wirksam unterbunden werden, so daß eine Feststellung des Verursachers anders als beim Telefon nicht unbedingt erforderlich ist. Unproblematisch ist die anonyme Veröffentlichung in moderierten Newsgroups, bei denen der Moderator die Verantwortung für die Beiträge übernimmt und mißbräuchliche Artikel nicht veröffentlicht; aber auch in unmoderierten Newsgroups gibt es legitime Gründe für eine anonyme Nutzung. Erforderlich ist die Anbieterkennzeichnung bei Informationsangeboten im WWW mit der Ausnahme privater Gelegenheitsangebote.

Kapitel 3

Technische Anforderungen

In diesem Kapitel werden die Maßnahmen zur Gewährleistung des Datenschutzes in Kommunikationsnetzen in den Zusammenhang der IT-Sicherheit eingeordnet. Am Modell einer Kommunikationsbeziehung (Sender, Empfänger, Angreifer) werden die sich aus dem Datenschutz ergebenden Anforderungen aufgezeigt und zu konkreten Internet-Diensten in Bezug gesetzt.

3.1 Sicherheit und Datenschutz

Datenschutz und IT-Sicherheit hängen eng zusammen. Der Schutz von Informationen vor unbefugtem Zugriff ist eine Voraussetzung des Datenschutzes. Letzterer ist jedoch ein über den Schutz der Vertraulichkeit hinausgehendes Konzept. Die Sammlung von Daten wird dabei grundsätzlich in Frage gestellt; sie sollte nur dann möglich sein, wenn es dafür einen guten Grund gibt [Rossum 1995].

Herkömmlich versteht man unter IT-Sicherheit die Abwesenheit von drei Arten von Grundbedrohungen [ITSEC 1991]:

- **Vertraulichkeit:** Schutz von Informationen vor unbefugter Kenntnisnahme.
- **Integrität:** Schutz von Informationen vor unbefugter Veränderung.
- **Verfügbarkeit:** Schutz vor Vorenthaltung von Informationen oder Betriebsmitteln.

Mittlerweile werden weitere Schutzziele betrachtet, darunter [Rannenberg 1996, CC 1996]:

- **Zurechenbarkeit:** Sicherstellung, daß für Vorgänge ein Verantwortlicher auszumachen ist.

- **Authentizität:** Gewährleistung, daß Informationen tatsächlich vom angegebenen Absender stammen.
- **Datenschutz:** Schutz der Identität des Nutzers vor Entdeckung und Mißbrauch durch andere [CC 1996].

[CC 1996] enthält eine umfangreiche Zusammenstellung funktionaler Sicherheitsanforderungen. Um aktuellen IT-Sicherheitsproblemen flexibel begegnen zu können, wird das Konzept der *Schutzprofile (protection profiles)* verwendet, die produktunabhängig ein Sicherheitskonzept dokumentieren. So soll für Standard-Sicherheitsprobleme eine anerkannte Lösung angeboten werden [Brauer 1996].

Die verschiedenen Schutzziele sind nicht immer konfliktfrei: Die Zurechenbarkeit geht verloren, wenn die Identität eines Nutzers aus Datenschutzgründen nicht bekannt ist. Daher muß anwendungsabhängig eine sinnvolle Balance gefunden werden. In Abschnitt 2.3.1 wurde diese Problematik in Bezug auf weltweite offene Netze behandelt.

3.2 Datenschutz

3.2.1 Personenbezogene Daten in Kommunikationsnetzen

Bei der Nutzung von Kommunikationsnetzen treten verschiedene Arten personenbezogener Daten in Erscheinung. Im Hinblick auf den Zweck der Diensteerbringung werden diese unterteilt in [Schaar 1996, Bundestag 1997]:

- **Bestandsdaten:** Kundendaten, die ein Netzbetreiber oder ein Anbieter von Telediensten dauerhaft speichert, um die Bereitstellung des Dienstes zu ermöglichen, beispielsweise Name und Anschrift, IP-Nummer oder E-Mail-Adresse des Kunden.
- **Inhaltsdaten:** die zu übertragenden Nutzdaten. Sofern sie nicht verschlüsselt übertragen werden, können sie auf dem gesamten Übertragungsweg zur Kenntnis genommen werden.
- **Verbindungsdaten:** Daten über die beteiligten Kommunikationspartner, Zeitpunkt und Dauer, übertragene Datenmengen usw. Verbindungsdaten werden zum Verbindungsaufbau und ggf. zur Abrechnung benötigt. Sie fallen bei allen an der Datenübertragung beteiligten Rechnern an.
- **Nutzungsdaten:** Daten, die bei der Nutzung eines Teledienstes, z. B. durch Interaktion mit dem Diensteanbieter, entstehen, beispielsweise Daten über Suchschritte oder vom Nutzer abgerufene Texte.
- **Abrechnungsdaten** werden aus den Verbindungsdaten und den Nutzungsdaten gewonnen.

Aus diesen Daten lassen sich Daten über den Nutzer gewinnen [Pfitzmann 1990]:

Den Nutzungsdaten lassen sich Informationen über die Interessen des Nutzers entnehmen **(Interessensdaten)**.

Verkehrsdaten sind Angaben darüber, wer zum welchem Zeitpunkt mit wem kommuniziert hat. Sie können aus den Verbindungsdaten gewonnen werden. Neben den Adressen in übertragenen Datenpaketen kann auch der Vergleich von Datenmengen und zeitlichen Zusammenhängen wie gleichzeitigem Öffnen und Schließen von Verbindungen *(Verkehrsanalyse)* Informationen über Kommunikationsbeziehungen ergeben.

Um das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung zu schützen, reicht die Vertraulichkeit der Inhaltsdaten somit nicht aus. Auch die Auswertung von Verkehrs- und Interessensdaten muß verhindert werden.

3.2.2 Prinzipien und Anforderungen

Um Bedrohungen der Vertraulichkeit zu vermeiden, sollen riskante Daten nach Möglichkeit gar nicht erst entstehen *(Datenvermeidung)*. Sie sollten nur dann anfallen, wenn sie für die Funktion des Systems erforderlich sind (vgl. Abschnitt 2.1.7). Die Erhebung von Vermittlungs- und Nutzungsdaten zu Abrechnungszwecken kann etwa durch die Verwendung digitaler Zahlungsverfahren wie vorbezahlter Chipkarten und digitalem Bargeld unnötig werden. Wo Daten für die Erbringung eines Dienstes erforderlich sind, kann die Verteilung auf mehrere Teile eines verteilten Systems (*Dezentralisierung)* die Attraktivität und die Folgen eines Mißbrauchs reduzieren [Rannenberg 1996].

Um das Entstehen personenbezogener Daten zu vermeiden, muß ein Kommunikationssystemen folgende Datenschutzanforderungen erfüllen [Pfitzmann 1990, Rannenberg 1995, CC 1996]:

Ist der Nutzer gegenüber dem Kommunikationspartner (z. B. einem Diensteanbieter) *anonym*, so entstehen dort keine personenbezogene Interessensdaten. Verfahren, die eine *unbeobachtbare Kommunikation* sicherstellen, verhindern das Entstehen von Verkehrsdaten. Verschiedene kommunikative Handlungen sollen *unverkettbar* sein, um zu verhindern, daß andere Wissen über Personen anzusammeln können, das deren Anonymität gefährden würde. Hat eine Telefonkarte beispielsweise eine eindeutige Nummer, kann der Telefonnetzbetreiber ein Kommunikationsprofil des Nutzers erstellen und ihn damit reidentifizieren. Häufig soll die Identität nicht erkennbar sein, aber trotzdem ein Bezug zu einem Individuum bestehen *(Pseudonymität)*. Dies ist beispielsweise erforderlich, um den Zugriff auf ein den individuellen Interessen des Nutzers entsprechend personalisiertes Informationsangebot zu ermöglichen, aber auch, wenn es nötig ist, Nutzer im Mißbrauchsfall zur Verantwortung zu ziehen.

3.3 Modell der Kommunikation

Verfahren für anonyme Kommunikation können im Internet in verschiedenen Situationen vom Zugriff auf WWW-Seiten bis zur Veröffentlichung von Artikeln in Newsgroups eingesetzt. Gemeinsam ist diesen Situationen, daß mindestens zwei Kommunikationspartner beteiligt sind, von denen jeweils einer unbeobachtet eine **Mitteilung** *(missive)* an den anderen übermitteln will. Dazu sendet er dem Kommunikationspartner oder einem Übermittler eine **Nachricht** *(message)*. Ein WWW-Zugriff besteht beispielsweise aus dem Senden einer Anfrage und dem Empfangen der Antwort; entsprechendes gilt für andere interaktive Dienste.

3.3.1 Rollen in einer Kommunikationsbeziehung

Eine **Instanz** ist jemand oder etwas, der Nachrichten sendet, empfängt oder verändert, z. B. eine Person oder ein Computer.

Sender ist in einer Kommunikationsbeziehung die Instanz, die legitimerweise eine Mitteilung überträgt. **Empfänger** ist diejenige Instanz, für die die übertragene Mitteilung bestimmt ist.

Unbeteiligte sind alle anderen Instanzen. Hierzu zählt auch der für die Nachrichtenübertragung verantwortliche Netzbetreiber.

Ein **vertrauenswürdiger Dritter** *(trusted third party)* ist eine Instanz, die eine Rolle in der Übertragung der Nachrichten übernimmt und auf deren korrektes Verhalten die Beteiligten vertrauen.

3.3.2 Angreifermodelle

Um die Sicherheit eines Verfahrens zu bewerten, werden verschiedene Angreifermodelle betrachtet. Als **Angreifer** wird dabei eine Instanz bezeichnet, die versucht, nicht für sie bestimmte Informationen oder Mitteilungen zu erhalten, falsche Mitteilungen zu senden oder die Erbringung eines Dienstes zu verhindern. Dies kann sowohl ein Außenstehender als auch ein Teilnehmer oder der Betreiber eines Netzdienstes sein.

Nach ihren Fähigkeiten werden verschiedene Angreifertypen unterschieden:

Ein **passiver** Angreifer kann einen Teil oder sämtliche Kommunikationsverbindungen abhören. Ein **aktiver** Angreifer kann zudem übertragene Nachrichten verfälschen, verzögern und unterdrücken und eigene Nachrichten übertragen, indem er versucht, als legitimer Sender zu erscheinen. Betrachtet wird auch die Möglichkeit, daß ein Teil der an der Kommunikation Beteiligten mit dem Angreifer *kooperiert* (**interner** Angreifer). Sich protokollkonform verhaltende Beteiligte werden auch als *ehrlich* bezeichnet. Angreifer werden weiter danach unterschieden, welche Berechnungen sie durchführen können, um etwa eine Verschlüsselung zu brechen.

3.4 Datenschutzanforderungen

Im folgenden werden die Datenschutzanforderungen Unbeobachtbarkeit und Unverkettbarkeit von Ereignissen sowie Anonymität und Pseudonymität von Instanzen beschrieben. Die Vertrauenswürdigkeit dieser Eigenschaften wird davon bestimmt, wie stark der bei der Definition zugrunde gelegte Angreifer ist [Pfitzmann 1990].

Als Ereignisse kommen beispielsweise das Senden einer Mitteilung oder das Abwickeln eines Geschäfts in Frage.

3.4.1 Anonymität

R_I bezeichne das Ereignis „Instanz I nimmt bei einem Ereignis die Rolle R wahr“. Eine Instanz I_0 heißt in einer Rolle R **anonym** [Pfitzmann 1990] bezüglich eines Ereignisses X, eines Angreifers E und einer Menge $\mathcal{A}$ von nicht mit E kooperierenden Instanzen (Anonymitätsmenge), wenn nach jeder für E möglichen Beobachtung B gilt: $\forall I \in \mathcal{A}\colon\ 0 < \mathrm{P}(R_I \mid B) < 1$. Dies kann auch für an X beteiligte Angreifer der Fall sein. Offensichtlich ist keine Anonymisierung möglich, wenn alle anderen Instanzen mit dem Angreifer kooperieren.

Man kann verschiedene Grade der Anonymität unterscheiden [Reiter 1997]:

- I_0 heißt **perfekt anonym** in der Rolle R bezüglich E und $\mathcal{A}$, wenn nach jeder für E möglichen Beobachtung B gilt: $\forall I \in \mathcal{A}\colon\ \mathrm{P}(R_I) = \mathrm{P}(R_I \mid B)$, d. h. die Beobachtung liefert E keine zusätzlichen Informationen darüber, wer die Rolle R wahrnimmt.
- I_0 ist **außer Verdacht** bezüglich R, wenn nach jeder für E möglichen Beobachtung B gilt: $\forall I \in \mathcal{A}\colon\ \mathrm{P}(R_{I_0} \mid B) \leq \mathrm{P}(R_I \mid B)$.
- I_0 ist **wahrscheinlich unbeteiligt** in Bezug auf R, wenn nach jeder für E möglichen Beobachtung B gilt: $\mathrm{P}(R_{I_0} \mid B) \leq \mathrm{P}(\bigcup_{I \in \mathcal{A} \setminus \{I_0\}} R_I \mid B)$.
- I_0 ist **möglicherweise unbeteiligt** in Bezug auf R, wenn nach jeder für E möglichen Beobachtung B eine nichttriviale Wahrscheinlichkeit besteht, daß eine andere Instanz die Rolle R wahrnimmt; $\mathrm{P}(R_{I_0} \mid B) < 1$.
- I_0 ist in der Rolle R **aufgedeckt**, wenn für eine für E mögliche Beobachtung B gilt: $\mathrm{P}(R_{I_0} \mid B) = 1$.
- I_0 ist in der Rolle R **beweisbar aufgedeckt**, wenn der E gegenüber anderen beweisen kann, daß I_0 die Rolle R wahrnimmt.

Je nach der bei einem Kommunikationsvorgang betrachteten Rolle spricht man von **Sender-Anonymität** oder **Empfänger-Anonymität.**

Im Falle bidirektionaler Kommunikation ist Sender-Anonymität nicht ohne Empfänger-Anonymität möglich, und umgekehrt. Der Sender einer anonymen Mitteilung muß auch anonym bleiben, wenn er eine Antwort empfängt; die Anonymität des Empfängers einer Nachricht muß erhalten bleiben, wenn er eine Antwort sendet [Waidner 1990]. Das betrifft nicht nur Dialoge zwischen Nutzern, sondern alle Internetdienste, für deren Nutzung ein Protokoll mit bidirektionaler Kommunikation nötig ist.

3.4.2 Unbeobachtbarkeit

Ein Ereignis X heißt **unbeobachtbar** [Pfitzmann 1990] bezüglich eines Angreifers E, wenn nach jeder für E möglichen Beobachtung B für die Wahrscheinlichkeit des Auftretens von X gilt: $0 < \mathrm{P}(X \mid B) < 1$. Ein Ereignis kann nur bezüglich Unbeteiligter unbeobachtbar sein.

X heißt **perfekt unbeobachtbar** bezüglich E, wenn für jede für E mögliche Beobachtung B gilt: $\mathrm{P}(X) = \mathrm{P}(X \mid B)$, d. h. daß die Beobachtung E keine zusätzlichen Informationen über X liefert.

Eine Instanz kann Mitteilungen nur unbeobachtbar senden oder empfangen, indem sie unabhängig von der Anzahl der Mitteilungen eine feste Anzahl von Nachrichten sendet bzw. empfängt.

Eine Kommunikationsbeziehung ist dann unbeobachtbar, wenn das Senden einer Nachricht nicht mit dem Empfangen einer bestimmten Nachricht durch eine Instanz in Verbindung gebracht werden kann. Man spricht daher auch von *Unverkettbarkeit von Sender und Empfänger.*

Wenn Kommunikation unbeobachtbar, aber nicht anonym erfolgen soll, können die Teilnehmer sich mit Hilfe digitaler Signaturen identifizieren.

3.4.3 Unverkettbarkeit

$M_{X,X'}$ bezeichne das Ereignis „Die Ereignisse X und X' stimmen bezüglich des Merkmals M überein“ (z. B. zwei Mitteilungen bezüglich ihres Senders). Zwei Ereignisse X und X' heißen bezüglich eines Merkmals M und eines Angreifers E **unverkettbar** [Pfitzmann 1990], wenn für nach jeder für E möglichen Beobachtung gilt: $0 < \mathrm{P}(M_{X,X'} \mid B) < 1$. Dies kann auch für an X und X' beteiligte Angreifer der Fall sein. X und X' heißen **perfekt unverkettbar,** wenn $\mathrm{P}(M_{X,X'} \mid B) = \mathrm{P}(M_{X,X'})$.

3.4.4 Pseudonymität

Anders als die vorgenannten Eigenschaften dienen Pseudonyme dem Datenschutz nicht direkt. Sie ermöglichen es, die Vorteile personenbezogener Nutzung mit denen der Anonymität zu kombinieren.

Ein Pseudonym ermöglicht z. B. eine personalisierte Nutzung von Telediensten, ohne daß die Identität Dritten bekannt wird. Die Verkettbarkeit der unter demselben Pseudonym durchgeführten Handlungen ist somit erwünscht. Sofern der Nutzer in unterschiedlichen Rollen verschiedene Pseudonyme verwendet, bleibt die Unverkettbarkeit von Vorgängen in anderen Rollen erhalten.

Ein **selbstgeneriertes Pseudonym** gibt einem Angreifer keine zusätzliche Information über die Identität, es erhält also die Anonymität.[1]

[1] In der hier verwendeten Ausdrucksweise (vgl. [Goldberg 1997]) ist eine *pseudonyme* Adresse also *anonym,* wenn die Identität des Nutzers nicht festzustellen ist. Teilweise werden die Begriffe *anonym* und *pseudonym* auch als Gegensätze verwendet.

Häufig ist es erwünscht, daß die Identität des Nutzers unter kontrollierten Bedingungen *aufgedeckt* werden kann. Kann das Pseudonym über eine Referenzliste mit der Identität des Nutzers zusammengeführt werden, spricht man von einem **Referenz-Pseudonym** [HmbDSB 1996]. Die Liste kann beispielsweise bei einem vertrauenswürdigen Dritten gespeichert werden. Wenn nur in Ausnahmefällen auf die Liste zugegriffen werden muß, kann sie so verteilt werden, daß die Zusammenarbeit mehrerer unabhängiger Stellen erforderlich ist, um an die Daten zu gelangen. Ein aufdeckbares Pseudonym ist nur in Bezug auf Angreifer anonym, mit denen der Geheimnisträger nicht kooperiert.

3.5 Datenschutzanforderungen bei Internet-Diensten

3.5.1 Sicherheit im Internet

Beim Entwurf der meisten im Internet eingesetzten Protokolle wurden Sicherheitsaspekte kaum berücksichtigt.

[Atkinson 1995] führt eine Sicherheitsarchitektur für das Internet-Protokoll ein. Damit sollen Integrität, Vertraulichkeit und Authentizität auf IP-Ebene sichergestellt werden. Der Schutz der Verfügbarkeit ist im Internet nicht gewährleistet. Das SSL-Protokoll [Freier 1996], das auf der Transportschicht ansetzt, um den Schutz der Inhaltsdaten zu gewährleisten, wird insbesondere für verschlüsselte Zugriffe auf WWW-Server genutzt. Für *remote login* und das Kopieren von Dateien wird das ebenfalls auf der Transportschicht basierende SSH-Protokoll [Ylönen 1997] verwendet. Um Vertraulichkeit und Authentizität von E-Mail zu erreichen, stehen Verfahren wie S/MIME und PGP [Dusse 1997, Zimmermann 1995] zur Verfügung.

Den Schutz der Verkehrsdaten gewährleistet jedoch keines dieser Verfahren. Quell- und Zieladressen sowie TCP-Portnummern bleiben bei Verschlüsselung auf der Transportschicht unverschlüsselt, bei der Verschlüsselung von E-Mail die Adressen von Absender und Empfänger und oft sogar die Betreff-Zeilen. Die Länge des Klartextes bleibt bei Stromchiffren erhalten, bei Blockchiffren wird sie zum nächstgrößeren Vielfachen der Blockgröße (üblicherweise 8 Bytes) aufgerundet. Bei WWW-Zugriffen über SSL ist somit der genutzte Server, die Länge des URL und der angeforderten Datei erkennbar. Viele HTML-Seiten enthalten Elemente, die den Browser zum automatischen Abruf weiterer Objekte veranlassen.[2] Anhand dieser Daten läßt sich die abgerufene Datei in vielen Fällen mit geringem Aufwand identifizieren [Wagner 1996].

3.5.2 E-Mail, Newsgroups

Zum Schutz vor der Erstellung von Kommunikationsprofilen sollte der Versand von E-Mail unbeobachtbar und auf Wunsch anonym erfolgen.

Soll Sender-Anonymität ermöglicht werden, müssen die den Nutzer identifizierenden Einträge aus dem Nachrichtenkopf (Header) entfernt werden. Neben Namen und

[2] Dies ist beispielsweise bei dem `src`-Attribut der Tags `<img>` und `<frame>` der Fall [Reiter 1997].

E-Mail-Adresse des Absenders weisen weitere Header-Einträge wie die Message-ID und `Received`-Zeilen, die den Weg der Nachricht wiedergeben, auf den absendenden Rechner hin. Andere Angaben wie die Betreff-Zeile beziehen sich auf den Inhalt und müssen erhalten bleiben.

Um Empfänger-Anonymität zu gewährleisten, müssen anonyme Rückadressen bestehen.

Die Interaktion zwischen anonymen Nutzern und anderen Beteiligten kann durch den Einsatz von Pseudonymen ermöglicht werden. Dabei sollte die Möglichkeit bestehen, in unterschiedlichen Rollen verschiedene Pseudonyme zu verwenden.

Bezüglich der Anonymisierung gilt für Usenet-Newsgroups Entsprechendes. Empfänger der anonymisierten Nachricht ist in dem Fall ein Newsserver, der sie dann im *flood-fill*-Verfahren weiterverbreitet.

3.5.3 WWW

Der Abruf von WWW-Seiten sollte unbeobachtbar und gegenüber dem Betreiber des Servers anonym erfolgen können. Erforderlich ist also bidirektionale anonyme Kommunikation mit kurzen Verzögerungszeiten. Auch hier müssen identifizierende Daten aus der Anfrage entfernt werden. Zusätzlich müssen Applets und vergleichbare Programme, die den Schutz des Nutzers gefährden könnten (siehe Abschnitt 2.1.3.1), aus der Antwort des Servers herausgefiltert werden.

Eine zunehmende Anzahl von WWW-Servern bietet personalisierte, auf die Vorlieben des einzelnen Nutzers zugeschnittene Angebote. Diese Dienste sollten unter Pseudonym nutzbar sein, wobei die Pseudonyme eines Nutzers für verschiedene Angebote unverkettbar sein sollten [Gabber 1997]. Auch wenn der Betreiber das Verhalten der Nutzer analysieren möchte, ist der Einsatz von Pseudonymen sinnvoll, damit – nicht personenbezogene – Nutzungsprofile erstellt werden können.

Auch Dienste für geschlossene Benutzergruppen, bei denen der Nutzer sich gegenüber dem Server identifizieren muß, sollten in Bezug auf Unbeteiligte unbeobachtbar genutzt werden können.

3.5.4 Anforderungen zur Benutzbarkeit

Damit sie ihren Sinn erfüllen, müssen Anonymisierungsverfahren nicht nur sicher sein, sondern auch effizient und einfach zu bedienen. Ein Verfahren, das den Nutzer zuverlässig anonymisiert, aber zu erheblichen Verzögerungen führt, kann für interaktive Dienste wie das WWW nicht eingesetzt werden. Auch ist die Übertragungskapazität des Netzes begrenzt. Daher sind gegebenenfalls Kompromisse zwischen Sicherheit und Effizienz des Verfahrens nötig.

Wenn sich die Anwendungssoftware zur Nutzung eines Internet-Dienstes eines Proxy-Servers bedienen kann, läßt sich die anonyme Nutzung des Dienstes benutzerfreundlich realisieren. Der Nutzer installiert dafür lokal ein Programm, das die für den Zugriff mittels eines Anonymisierungsdienstes nötigen Schritte durchführt und für die Anwendungssoftware als Proxy fungiert. Anonyme Zugriffe sind daraufhin für ihn transparent über die gewohnte Benutzerschnittstelle möglich [Syverson 1997, McCoy 1997].

Wenn Anonymisierungsdienste kommerziell betrieben werden, muß sichergestellt sein, daß der Betreiber für seinen Dienst bezahlt wird, obwohl die Nutzer anonym bleiben. Dieses Problem kann durch den Einsatz anonymer digitaler Zahlungssysteme gelöst werden.

3.6 Grenzen der technischen Anonymisierung

Auch wenn ein Anonymisierungsverfahren selbst sicher ist, bestehen weiterhin Möglichkeiten, Nutzer zu identifizieren.

Voraussetzung für die Anonymisierung ist, daß der Nutzer ein vertrauenswürdiges Endgerät verwendet. Wenn ein Angreifer durch maliziöse Software wie Viren oder Trojanische Pferde an Informationen über den Nutzer gelangen kann, bieten Anonymisierungsverfahren keinen Schutz. Die Verwendung eines unsicheren Betriebssystems gefährdet die Anonymität des Nutzers auch dann, wenn das verwendete Anonymisierungsverfahren selbst sicher ist.

Durch das Unterbrechen von Kommunikationsverbindungen *(denial-of-service-Angriffe)* lassen sich einzelne Nutzer aus der Anonymitätsmenge entfernen. Wird beispielsweise eine anonyme Nachricht beobachtet, kommen die Nutzer nicht als Sender in Frage, deren Kommunikationsverbindung zum Absendezeitpunkt gestört wurde. Sind mehrere Kommunikationsvorgänge eines Nutzers verkettbar, kann ein aktiver Angreifer einen von n möglichen Nutzern in $O(\log n)$ Schritten identifizieren, indem er die Menge der Nutzer jeweils halbiert [Pfitzmann 1990]. Mit kryptographischen Methoden lassen sich *denial-of-service*-Angriffe nicht verhindern. Da auch die im Internet eingesetzte Kommunikationstechnik keinen Schutz gegen Angriffe auf die Verfügbarkeit bietet, kann die Anonymität der Nutzer nur geschützt werden, indem im Fall eines solchen Angriffs die anonyme Nachrichtenübertragung für alle Nutzer unterbrochen wird *(fail-stop*-Verfahren) [Waidner 1990]. Bei diesem Verfahren können einzelne Teilnehmer und fehlerhafte Netzkomponenten die Kommunikation nachhaltig stören. Um die Nutzbarkeit des Verfahrens nicht durch häufige Unterbrechungen einzuschränken, muß dann versucht werden, Teilnehmer, bei denen die Fehlerrate übermäßig hoch ist, zu erkennen und auszuschließen. Eine andere Möglichkeit besteht darin, das Fehlen von Nachrichten erst im Nachhinein zu untersuchen, statt Angriffe von vornherein zu verhindern, so daß der Angreifer gegebenenfalls verfolgt werden kann [Pfitzmann 1989].

Die übertragenen Daten selbst erlauben oft Rückschlüsse auf den Urheber. Im Fall der Sprachübertragung ist es möglich, Sprecher automatisch zu identifizieren. Stimmerkennungssysteme werden zum Beispiel in der Telefonüberwachung eingesetzt.

Auch der Autor eines schriftlichen Dokuments ist oft an stilistischen Merkmalen zu erkennen. Dafür werden beispielsweise statistische Eigenschaften wie der Reichtum des Wortschatzes und der verwendeten grammatischen Konstruktionen eines Textes analysiert [Horton 1994]. Anonyme Autoren konnten auf diese Weise in verschiedenen Fällen identifiziert werden.

Kapitel 4

Einfache Anonymisierungsverfahren

4.1 Anonymisierung von WWW-Logfiles

Als einfache Maßnahme für eine datenschutzkonforme Gestaltung von WWW-Angeboten wurde eine Modifikation der Server-Software vorgeschlagen, um die in Logfiles gespeicherten Daten zu anonymisieren [Blome 1996].

Rechnername und Internet-Adresse des Abrufers lassen häufig auf die Identität schließen, sind also personenbezogene Daten (siehe Abschnitt 2.1.1.1). Statt diese Daten zu speichern, protokolliert ein modifizierter Server die Domain-Adresse ohne den Rechnernamen und nur die ersten drei der vier Oktette einer IP-Adresse. Die nicht gespeicherten Adreßbestandteile werden durch die Zeichenfolge `xxx` ersetzt. Damit ist weiterhin feststellbar, aus welchem Netz der Zugriff erfolgt ist; statistische Auswertungen über die Nutzung des WWW-Angebots sind also möglich. Die gespeicherten Daten sind aber nicht personenbezogen.

Mit diesem Verfahren kann ein WWW-Anbieter seine datenschutzrechtliche Pflicht zur Datenvermeidung erfüllen. Der Nutzer hat allerdings keine Möglichkeit, zu überprüfen, ob seine Daten anonymisiert gespeichert werden. Gegen Anbieter, die sich rechtswidrig verhalten oder ihr Angebot in einem Land ohne vergleichbare Datenschutzvorschriften betreiben, bietet das Verfahren keinen Schutz.

Im internationalen Rahmen kann es sinnvoll sein, daß die Einhaltung von Richtlinien zum Umgang mit persönlichen Daten von einer unabhängigen Organisation überprüft und zertifiziert wird, so daß die Anbieter ihr Angebot mit einem entsprechenden Logo kennzeichnen können [Damker 1997]. Dieses Vorgehen ist allerdings auf die freiwillige Selbstverpflichtung der Anbieter und die Unabhängigkeit der Zertifizierungsstelle angewiesen.

4.2 Anonymisierung von WWW-Zugriffen

Mit der Hilfe eines vertrauenswürdigen Dritten kann der Nutzer gegenüber dem Anbieter anonym bleiben. *The Anonymizer* ist ein durch Beiträge der Nutzer finanzierter WWW-Anonymisierungsdienst in den USA, der auf diesem Prinzip beruht [Boyan 1997]. Der *Lucent Personalized Web Assistant* [Gabber 1997] bietet eine entsprechende Funktion und erlaubt zusätzlich pseudonymen Zugriff auf personalisierte WWW-Angebote. Auch die frei verfügbare Proxy-Software Squid bietet die Möglichkeit, Zugriffe zu anonymisieren.

4.2.1 Verfahren

Um unnötige Mehrfachzugriffe auf entfernte WWW-Server einzusparen, werden Proxy-Server eingesetzt. Der Browser des Anwenders richtet seine Anfrage nicht direkt an den Server, sondern an seinen lokalen Proxy. Dieser leitet die Anfrage sowie die Antwort des Servers weiter, speichert die fremde Seiten aber auch für eine gewisse Zeit, damit er weitere Zugriffe auf diese Seite selbst bedienen kann.

Dieses Prinzip kann auch zur Anonymisierung eingesetzt werden. Der Proxy entfernt dazu die identifizierenden Daten aus der Anfrage. Der WWW-Server kann sie somit nur noch der Gruppe der Nutzer dieses Proxy-Servers zuordnen, nicht mehr einer einzelnen Person.

Den *Anonymizer*-Dienst kann der Nutzer in seinem Browser als Proxy-Server eintragen; daraufhin erfolgen alle WWW-Zugriffe anonymisiert. Für den Fall, daß er nur auf bestimmte WWW-Server anonym zugreifen will, besteht auch die Möglichkeit, auf den Anonymisierungsdienst wie auf andere WWW-Server zuzugreifen. Die Adresse des Objekts wird dabei im lokalen Teil des URL übergeben, indem dem URL der gewünschten Seite der Text `http://www.anonymizer.com:8080/` vorangestellt wird. Die im abgerufenen Dokument enthaltene Hypertextlinks werden dann automatisch in diese Form gebracht, so daß auch Folgezugriffe anonym bleiben. Elemente wie Java-Applets, die zur Aufdeckung der Identität führen könnten, werden aus der Antwort des Servers herausgefiltert.

Der Squid-Proxy beherrscht zwei verschiedene Strategien: Entweder werden bekannte personenbezogene Daten wie die `From`-Zeile und Cookies aus der Anfrage entfernt, oder es werden nur die als harmlos erkannten Daten übertragen. Bei der ersten Methode besteht die Gefahr, daß zukünftige Erweiterungen zur Aufdeckung der Identität führen können; der anderen fehlt dagegen die Flexibilität gegenüber Neuerungen.

4.2.2 Sicherheit

Durch dieses Verfahren ist der Nutzer dem WWW-Anbieter gegenüber anonym. Da `Referer`-Header und Cookies entfernt werden, können die Zugriffe nur eingeschränkt verkettet werden; die Möglichkeit besteht durch zeitliche Zusammenhänge und in den URLs kodierte Zustandsinformationen aber weiterhin.

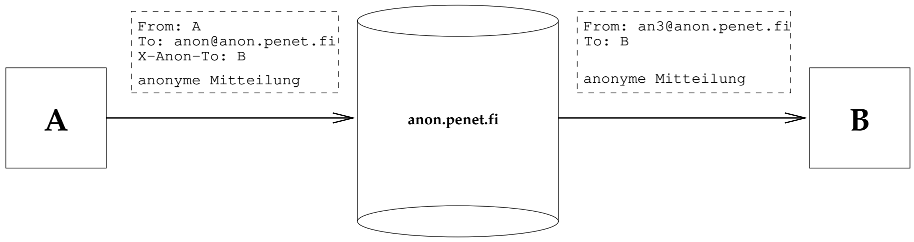


Abbildung 4.1: Funktionsweise des Anon-Servers

Der Nutzer eines Proxy-Servers muß damit rechnen, daß alle seine WWW-Zugriffe vom Proxy protokolliert werden. Im Vergleich zu Zugriffen ohne Proxy verliert er somit an Unbeobachtbarkeit. Dieses Verfahren erfordert daher, daß der Proxy-Betreiber vertrauenswürdig ist.

Die Übertragung zwischen dem Nutzer dem Anonymisierungsdienst kann mit SSL verschlüsselt werden. Die Längen der Requests (und damit der angeforderten URLs) und der übertragenen Dateien sind damit aber weiterhin erkennbar [Wagner 1996]. Der verschlüsselten Übertragung der Datei geht ein – üblicherweise unverschlüsselter – Zugriff des Anonymisierungsdienstes auf die nachgefragte Datei voraus. Kann der Angreifer auch die Verbindung zwischen dem Anonymisierungsdienst und dem Server abhören, ist also eine in den meisten Fällen eindeutige Zuordnung möglich. Auch wenn der Angreifer nur die Verbindung zwischen dem Nutzer und dem Anonymisierungsdienst abhört, kann er durch die Anwendung von WWW-Suchtechniken möglicherweise Dateien anhand ihrer Längen identifizieren. Unbeobachtbarkeit gegenüber einem passiven Angreifer ist in diesem Fall also nur eingeschränkt, ohne Verschlüsselung gar nicht gegeben.

4.3 Der Anon-Server anon.penet.fi

Der inzwischen geschlossene *Anon-Server* `anon.penet.fi` ermöglichte es, E-Mail und Usenet-Artikel unter einem Pseudonym zu versenden [Helsingius 1993]. Das Verfahren bietet Sender- und Empfängeranonymität gegenüber dem Kommunikationspartner.

4.3.1 Verfahren

Der Nutzer sendet seine Mitteilung unverschlüsselt per E-Mail an `anon@anon.penet.fi`. Der eigentliche Empfänger wird in einer zusätzlichen Header-Zeile `X-Anon-To:` angegeben; Adressat kann eine E-Mail-Adresse, der Name einer Newsgroup oder eine auf dem Anon-Server bestehende Alias-Adresse sein.

```
Path: ulf.mali.sub.org!malihh!news.Hanse.DE!news.rrz.uni-hamburg.de!news.dkrz.d
e!news.dfn.de!xlink.net!bloom-beacon.mit.edu!news2.near.net!howland.reston.ans.
net!vixen.cso.uiuc.edu!news.uoregon.edu!news.algonet.se!news.hebel.net!news.tel
e.fi!news.csc.fi!news.eunet.fi!anon.penet.fi
Newsgroups: de.test
Message-ID: <003126Z14061996@anon.penet.fi>
From: an577290@anon.penet.fi (Theobald Tiger)
X-Anonymously-To: de.test
Organization: Anonymous forwarding service
Reply-To: an577290@anon.penet.fi
Date: Fri, 14 Jun 1996 00:20:20 UTC
Subject: Hallo
Lines: 7

Guten Tag!

--------------------------------------------------------------------------
To find out more about the anon service, send mail to help@anon.penet.fi.
Due to the double-blind, any mail replies to this message will be anonymized,
and an anonymous id will be allocated automatically. You have been warned.
Please report any problems, inappropriate use etc. to admin@anon.penet.fi.
```

Abbildung 4.2: Eine (fiktive) Nachricht unter Pseudonym

Der Server entfernt aus dem Nachrichten-Header die Einträge, die es ermöglichen können, den Absender zu identifizieren. Nur die auf den Nachrichteninhalt bezogenen Angaben wie der Betreff bleiben erhalten.

Wenn der Nutzer noch keine Alias-Adresse hat, wird ihm eine neu erzeugte Adresse der Form `anNNNN@anon.penet.fi` zugewiesen. Zusätzlich besteht die Möglichkeit, ein Pseudonym für das Namens-Feld der Nachricht frei zu wählen. Die Alias-Adresse wird zusammen mit der tatsächlichen Adresse in einer Datenbank gespeichert; es handelt sich somit um ein Referenzpseudonym. Diese Adresse wird in die `From`-Zeile der Nachricht eingesetzt. Nach Überprüfung einer Größenbegrenzung und Abgleich des Empfängers mit einer Sperrliste wird der Nachricht ein Hinweistext angefügt, dann wird sie an den Empfänger weitergeleitet.

Über die Alias-Adresse kann der Empfänger auf die Nachricht antworten, ohne die Identität des Absenders zu kennen. Antworten an eine Alias-Adresse werden automatisch ebenfalls anonymisiert. Somit findet auch der weitere Austausch von Nachrichten über den Anon-Server statt, und keiner der Beteiligten erfährt die Identität des anderen.

Ein Nutzer, der den Inhaber einer Alias-Adresse erreichen will, ohne selbst unter Pseudonym aufzutreten, kann seine Nachricht an eine Adresse der Form `naNNNN@anon.penet.fi` mit der entsprechenden Nummer adressieren; sie wird dann unverändert an den Empfänger weitergeleitet.

4.3.2 Sicherheit

Das Verfahren bietet nur relativ geringen Schutz, war aber aufgrund der einfachen Benutzung sehr beliebt. Die Identität des Nutzers kann durch Bedienfehler, passive oder aktive Angriffe auf die Kommunikationsverbindung oder durch einen Angriff auf die Datenbank des Servers offengelegt werden.

4.3.2.1 Bedienfehler

Ein Nutzer kann die eigene Identität durch Bedienfehler unbeabsichtigt preisgeben. Da Antworten an anonymisierte Nachrichten ebenfalls anonymisiert werden, kann der Nutzer die an seine Alias-Adresse gesandte E-Mail einfach mit der Antwortfunktion des Mail-Programms beantworten; der Austausch aller Nachrichten findet über den Anon-Server statt. Wenn er aber über die `naNNNN`-Adressierung eine nicht anonymisierte Nachricht erhält, muß er daran denken, die Antwort mit einer `X-Anon-To`-Anweisung versehen an den Anon-Server zu adressieren. Ansonsten wird sie direkt zugestellt, und der Empfänger erfährt seine Identität.

Wenn ein Nutzer eine Nachricht beantwortet, als deren Absender eine Alias-Adresse angegeben ist, leitet der Anon-Server die Antwort mit dem Pseudonym des Nutzers versehen an den Inhaber der Alias-Adresse weiter. Falls der Nutzer nicht bemerkt, daß seine Antwort an eine Alias-Adresse geschickt wird und deshalb in der Antwort seinen Namen oder einen anderen Bezug zu seiner Person angibt, erfährt der Empfänger die Verknüpfung von Pseudonym und Identität [anon 1993].

Erhält ein Nutzer, für den ein Pseudonym registriert ist, eine anonyme Nachricht an seine normale Adresse, muß er seine Antwort an die `naNNNN`-Adresse des Kommunikationspartners senden. Ansonsten würde dieser sein Pseudonym erfahren.

4.3.2.2 Keine rollenbasierten Pseudonyme

Jedem Nutzer ist zu einem gegebenen Zeitpunkt nur ein Pseudonym zugeordnet. Die Möglichkeit, für unterschiedliche Rollen verschiedene Pseudonyme zu verwenden, besteht nicht. Daher ist es weiter möglich, Nutzerprofile zu erstellen. Wenn die Identität des Nutzers durch einen Bedienfehler oder einen Angriff bekannt wird, steht das gesamte Profil personenbezogen zur Verfügung. Denkbar ist auch, daß die im Profil enthaltenen Interessensdaten selbst zur Reidentifikation ausreichen.

4.3.2.3 Passive Angriffe

Da die Nachrichten nicht verschlüsselt werden, können sie auf allen an der Übertragung beteiligten Systemen gelesen werden (siehe Abschnitt 2.1.3.2). Vor der Anonymisierung sind in der Nachricht beide Kommunikationspartner erkennbar. Ein passiver Angreifer kann also feststellen, welche anonymen Nachrichten der Nutzer versendet.

Wer Nachrichten sowohl auf der Sender- als auch auf der Empfängerseite abhören kann, kann feststellen, welches Pseudonym zu dem Absender gehört. Das ist beispielsweise für den Systembetreiber der Fall, wenn beide Beteiligten derselben Organisation angehören. Auch wenn die Nachricht an eine Newsgroup gerichtet ist, reicht es, das System des Absenders zu kontrollieren. Zur Aufdeckung eines Pseudonyms können schon die Angaben zu Absender, Empfänger und Zeit einer Nachricht, wie sie in einem Mail-Logfile gespeichert sind, ausreichen.

4.3.2.4 Aktive Angriffe

Die Zuordnung der Alias-Adresse erfolgt anhand der Absenderadresse in der `From`-Zeile der Nachricht. Da es (durch Ändern der Voreinstellungen des Mail-Clients) ohne weiteres möglich ist, eine falsche Adresse zu verwenden, werden aktive Angriffe möglich, die ohne Zugriff auf die Kommunikationsverbindungen auskommen. Wenn der Angreifer eine Nachricht mit einer gefälschten `From`-Zeile an den Server sendet und z. B. an eine Newsgroup weiterleiten läßt, kann er der anonymisierten Nachricht das Pseudonym des Betroffenen entnehmen.

Entsprechend ist es möglich, die zu einem Pseudonym gehörende Identität herauszufinden, wenn nur ein begrenzter Personenkreis als Absender in Frage kommt. Der Angreifer führt denselben Angriff mit allen in Frage kommenden Adressen durch, wobei er die Adresse oder eine andere eindeutige Zeichenkette jeweils im – vom Server unverändert weitergeleiteten – Nachrichten-Text wiedergibt. Diejenige Nachricht, die unter dem fraglichen Pseudonym erscheint, gibt dem Angreifer Auskunft über die Identität des gesuchten Nutzers. Um diese Angriffe zu verhindern, wurde zusätzlich die Möglichkeit eingeführt, das Pseudonym mit einem Paßwort zu schützen.

4.3.2.5 Zentrale Datenbank

Die größte Schwäche des Verfahrens stellt die zentrale Datenbank dar. Die Nutzer müssen nicht nur darauf vertrauen, daß der Betreiber des Dienstes die Daten nicht freiwillig oder unter Zwang an Unbefugte herausgibt, sondern auch darauf, daß das System gegen alle Einbruchsversuche gesichert ist [Goldberg 1997]. Als der Server geschlossen wurde, waren dort Datensätze von insgesamt 800 000 Personen gespeichert, von denen viele dringend darauf angewiesen waren, daß ihre Identität vertraulich blieb. Diese Datenbank wurde daher zum Ziel vieler Angriffe. 1996 wurden täglich mehr als 20 ernsthafte Versuche beobachtet, in das System einzubrechen [Borchers 1997].

1995 beschuldigte Scientology einen Kritiker der Organisation, Dokumente von einem Computer der Organisation gestohlen und über den Anon-Server veröffentlicht zu haben. Der Server wurde deshalb – ohne richterlichen Beschluß – von der finnischen Polizei durchsucht. Der Betreiber Johan Helsingius mußte die tatsächliche E-Mail-Adresse des Nutzers herausgeben. Obwohl die Ermittlungen ergaben, daß weder Helsingius noch der amerikanische Nutzer eine Straftat begangen hatten, gab die finnische Polizei die Adresse an Scientology weiter.

Im Juni 1996 wandte sich die finnische Polizei wieder an Helsingius, um die Namen zweier Nutzer zu erfahren, die Scientology-Dokumente veröffentlicht hatten. Nachdem Helsingius' Einspruch dagegen am 22. August in erster Instanz mit der Begründung abgelehnt wurde, das Briefgeheimnis gelte nicht für E-Mail, stellte Helsingius den Dienst aufgrund der unsicheren Rechtslage ein [Newman 1996].

4.3.3 Bewertung

Viele Probleme dieses Verfahrens hängen eng mit der einfachen Anwendbarkeit zusammen. Die Verwendung rollenbasierter Pseudonyme würde erfordern, daß der Nutzer für jede Nachricht bewußt ein Pseudonym auswählt. Damit würden auch die in Abschnitt 4.3.2.1 beschriebenen Fehlerquellen ausgeschlossen. Der Normalfall, daß ein Nutzer unter Pseudonym eine Frage stellt und daraufhin unter diesem Pseudonym in einen Dialog mit anderen Teilnehmern tritt, wäre dadurch jedoch etwas umständlicher zu handhaben.

Um Antwortadressen ohne eine zentrale Datenbank zur Verfügung zu stellen, sind aufwendigere Verfahren erforderlich. Das Abhören der Mitteilungen läßt sich nur durch den Einsatz von Verschlüsselungsverfahren wirksam verhindern. Eine erheblich höhere Sicherheit als `anon.penet.fi` können vergleichbar einfache Verfahren also nicht bieten. Um ein Verfahren mit höherer Sicherheit entsprechend einfach bedienbar zu gestalten, ist der Einsatz spezieller Software auf der Seite des Nutzers erforderlich.

4.4 Cypherpunk-Remailer

Cypherpunk-Remailer lösen einige der im vorigen Abschnitt genannten Probleme. Sie beruhen ebenfalls auf dem Prinzip des Anonymisierens und Weiterleitens. Ergänzt wird es durch die Möglichkeit, Verschlüsselung zur Gewährleistung der Vertraulichkeit und Remailer-Sequenzen zur Dezentralisierung zu verwenden. Die im Internet nutzbaren Cypherpunk-Remailer verschiedener Betreiber werden mit Angaben zu ihrer Zuverlässigkeit in einer zentralen Liste [EFGA 1998] aufgeführt.

4.4.1 Verfahren zur Sender-Anonymität

Im einfachsten Fall schickt der Nutzer seine Nachricht mit einer zusätzlichen Header-Zeile, die die Zeichenkette `Anon-To:` und Adresse des Empfängers enthält, an den Remailer. Dort werden die personenbezogenen Header-Zeilen entfernt und ein erläuternder `Comments`-Eintrag in den Header eingefügt. Nach Abgleich mit einer Sperrliste wird die anonymisierte Nachricht an den Empfänger weitergeleitet.

Um die Zuordnung von Nachrichten anhand der Sende- und Empfangszeitpunkte zu erschweren, ist es möglich, in einen weiteren Header-Eintrag eine Verzögerungszeit anzugeben.

Zum Schutz gegen Abhören kann das Verschlüsselungsprogramm PGP eingesetzt werden. Dazu werden die für den Remailer bestimmten Header-Zeilen sowie die eigentliche Mitteilung mit dem öffentlichen Schlüssel des Remailers verschlüsselt. Die Header-Zeile `Encrypted: PGP` weist den Remailer an, die Nachricht mit PGP zu entschlüsseln und dann gemäß der entschlüsselten Header weiterzubearbeiten.

Statt die verschlüsselte Nachricht sofort an den Remailer zu senden, kann der Nutzer diesen Schritt für weitere Remailer wiederholen. Dadurch entsteht eine mehrfach verschlüsselte Nachricht, von der dann jeder Remailer eine Schicht der Verschlüsselung entfernt und die resultierende Nachricht an den folgenden Remailer weiterleitet (siehe Abbildung 4.3). Bei Verwendung einer solchen Sequenz von Remailern ist der

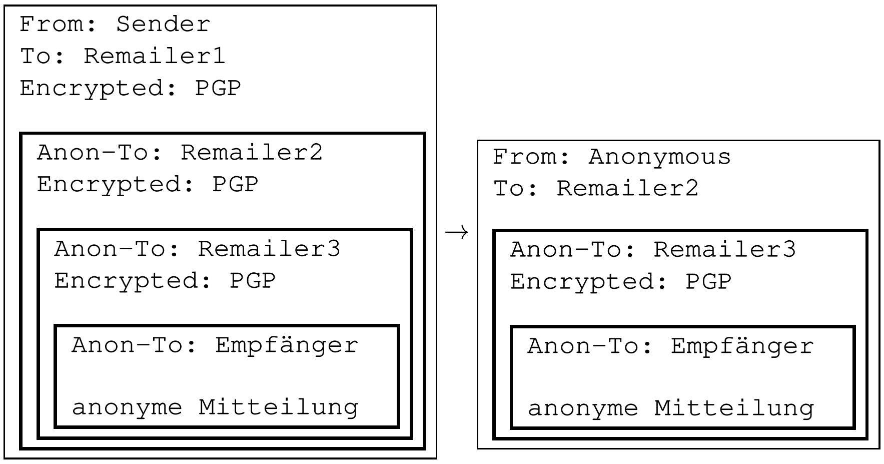


Abbildung 4.3: Anwendung einer Remailer-Sequenz

Absender nur dem ersten und der Empfänger (sowie bei unverschlüsselten Nachrichten der Inhalt) nur dem letzten Remailer bekannt.[1]

4.4.2 Verfahren zur Empfänger-Anonymität

Um E-Mail anonym empfangen zu können, erzeugt der Nutzer einen Rückadreß-Block *(reply block):* eine verschlüsselte Nachricht, die von einer Remailer-Sequenz an ihn selbst weitergeleitet werden soll. Diese Nachricht enthält also die notwendige Information, um den Nutzer anonym zu erreichen und kann einem Kommunikationspartner als Rückadresse dienen [Goldberg 1997].

Der Kommunikationspartner sendet die eigentliche Nachricht zusammen mit der Rückadreß-Information an den ersten Remailer der Sequenz. Die Remailer entschlüsseln die Nachricht und leiten sie an den Empfänger weiter; der nicht verschlüsselte Teil mit der eigentlichen Nachricht wird dabei unverändert weitergeleitet. Der Nutzer hat beim Erzeugen des Rückadreß-Blocks zusätzlich die Möglichkeit, einen Schlüssel zu spezifizieren, mit dem die weiterzuleitende Nachricht symmetrisch verschlüsselt wird.

4.4.3 Pseudonymität

Wenn der Nutzer eine pseudonymen E-Mail-Adresse verwendet, können andere mit ihm kommunizieren, ohne sich mit der Rückadreß-Information zu befassen. Pseudonyme werden bei diesem System, ähnlich wie bei `anon.penet.fi`, von einem Server *(„nym server“)* gespeichert. Statt der Adresse des Nutzers enthält die Datenbank aber nur den Rückadreß-Block. Die Kommunikation mit dem Pseudonym-Server erfolgt

[1] Dieses Verfahren ist an das in Kapitel 6 behandelte Mix-Netz angelehnt, hat in dieser Form aber noch Sicherheitsprobleme.

verschlüsselt. Durch die Verwendung einer Remailer-Sequenz kann der Nutzer dem Server gegenüber anonym bleiben.

Um ein neues Pseudonym zu erzeugen, sendet der Nutzer dem Server eine Nachricht mit dem gewünschten Pseudonym, einem für dieses Pseudonym generierten PGP-Schlüssel[2] und einem Rückadreß-Block. Nach der Einrichtung der Adresse kann der Nutzer pseudonyme Mitteilungen verschicken, indem er sie PGP-verschlüsselt und -signiert anonym an den Server sendet. Anweisungen ohne gültige Signatur ignoriert der Server. Für die pseudonyme Adresse eintreffende Nachrichten werden verschlüsselt und an die anonyme Rückadresse weitergeleitet.

4.4.4 Sicherheit

Der Nutzer ist bezüglich seiner Kommunikationspartner und des Pseudonym-Servers anonym, das Senden von Mitteilungen unter verschiedenen Pseudonymen unverkettbar.

Einzelne Remailer-Betreiber können das Senden bzw. das Empfangen einer Nachricht beobachten. Trotzdem ist die Kommunikationsbeziehung zwischen Sender und Empfänger für einzelne Remailer unbeobachtbar.

4.4.4.1 Passive Angriffe

Ein Angreifer, der Kommunikationsverbindungen abhört oder mit Remailern kooperiert, erhält Informationen über die Länge der übertragenen Nachrichten. PGP-Verschlüsselung bietet dagegen keinen Schutz (die bei PGP vorgesehene Kompression kann vernachlässigt werden, da bereits verschlüsselte Nachrichten nicht komprimierbar sind und ein Angreifer unverschlüsselte Nachrichten ebenfalls komprimieren kann). Auf dem Weg durch die Remailer-Sequenz wird eine Nachricht kleiner, da jeder Remailer eine Schicht der Verschlüsselung mit den dazugehörigen Adreß-Informationen entfernt.

Ein Angreifer, der die ankommenden und abgehenden Nachrichten eines Remailers beobachtet, kann die Nachrichten daher anhand ihrer Länge zuordnen. Unsicherheit besteht für ihn nur über die Zuordnung von gleichzeitig eintreffenden Nachrichten annähernd gleicher Länge. Bei der Verwendung von Verzögerungszeiten wird die Zuordnung erschwert, wenn während der Wartezeit weitere Nachrichten der entsprechenden Länge eintreffen; ansonsten ist sie nutzlos [Cottrell 1995, Franz 1997].

Bezüglich eines Angreifers, der *alle* Kommunikationsverbindungen abhört, bieten Cypherpunk-Remailer somit fast keinen Schutz. Fast immer wird nur eine geringe Anzahl von Zuordnungen zwischen Absendern und anonymisierten Nachrichten möglich sein. Verwendet der Nutzer ein Pseudonym in mehreren Nachrichten, kann der Angreifer die Schnittmenge der jeweils in Frage kommenden Absender bilden und so nach einigen Beobachtungen eine eindeutige Zuordnung erhalten.

[2] Bei einer anderen Implementation ein Paßwort, das zur Authentisierung und als geheimer Schlüssel für die Kommunikation verwendet wird.

Wenn der Angreifer nur einen *Teil* der Verbindungen abhört, beispielsweise – wie in Abschnitt 4.3.2.3 betrachtet – auf Sender- und Empfängerseite, wird die Analyse durch die Unsicherheit über die Nachrichten anderer Teilnehmer zwar erschwert, aber nicht unmöglich. Beobachtet der Angreifer häufiger, als nach seinem Modell vom Verhalten der anderen Teilnehmer zu erwarten wäre, daß ein Nutzer eine Nachricht an einen Remailer sendet und daß innerhalb einer gewissen Zeitspanne eine kürzere anonyme Nachricht empfangen wird, so ist der Nutzer nur noch möglicherweise unbeteiligt an dieser Nachricht. Eine falsche Vermutung ist widerlegt, sobald eine anonyme Nachricht beobachtet wird, ohne daß der Nutzer vorher eine größere Nachricht an einen Remailer geschickt hat. Für eine richtige Vermutung geht die Wahrscheinlichkeit der Zuordnung mit der Anzahl der Beobachtungen gegen 1.

Gegen Angreifer, die die Kommunikationsverbindung zwischen Nutzer und Remailer *nicht* abhören können, ist das System sicher. Angriffe auf die Pseudonym-Datenbank selbst stellen keine zusätzliche Gefahr für die Anonymität des Nutzers dar, weil die Erreichbarkeits-Informationen auf eine Sequenz von Remailern verteilt sind.

4.4.4.2 Aktive Angriffe

Im Fall der Empfänger-Anonymität kann ein Angreifer dem Nutzer Nachrichten beliebiger Länge und Anzahl schicken. Wenn er beobachten kann, wer Nachrichten dieser Länge und Anzahl erhält, ist der Nutzer aufgedeckt.

Ein entsprechender aktiver Angriff ist im Fall der Sender-Anonymität möglich, wenn der Angreifer Zugriff auf eine verschlüsselte Nachricht hat, die der Sender an einen Remailer geschickt hat. Der Angreifer kann diese Nachricht beliebig oft an den Remailer schicken *(Replay-Angriff)* und beobachten, wo eine Nachricht in entsprechender Anzahl ankommt.

Weil zu anonymisierende Nachrichten dasselbe Format wie Rückadreß-Blöcke haben, aber keine Anweisung zum Verschlüsseln des angehängten Textes enthalten, kann der Angreifer auch einen beliebigen Text an die Nachricht anhängen und beobachten, welche Remailer und schließlich welcher Nutzer die Nachricht erhält. Da der Absender bekannt ist, ist die Nachricht damit deanonymisiert.

4.4.5 Bewertung

Die zu übertragenden Nachrichten sind geringfügig länger; die Anzahl zusätzlicher Datenübertragungen ergibt sich aus der Zahl der eingesetzten Remailer. Die Benutzung der Cypherpunk-Remailer kann durch den Einsatz einer Windows-Oberfläche vereinfacht werden, die die Verschlüsselungsschritte steuert. Der zusätzliche Aufwand für dieses Verfahren ist damit für die meisten Anwendungen akzeptabel.

Gegen Angreifer, die die Kommunikation zwischen Nutzer und Remailer nicht systematisch überwachen, bieten Cypherpunk-Remailer einen besseren Schutz als der Anon-Server `anon.penet.fi`. Sie haben allerdings deutliche Schwachstellen.

4.5 Crowds

Das *Crowds*-System [Reiter 1997] ermöglicht anonyme WWW-Zugriffe. Es bietet eine effiziente Möglichkeit, Anonymität gegenüber dem WWW-Server zu erreichen, wobei die Kommunikationsbeziehung für lokal abhörende Angreifer unbeobachtbar bleibt, schützt aber nicht gegen globales Abhören.

4.5.1 Verfahren

Der Nutzer ist Mitglied einer als *Crowd* bezeichneten Gruppe. Jeder Teilnehmer der Crowd betreibt einen *Jondo* genannten Prozeß. Um einen anonymen WWW-Zugriff durchzuführen, sendet der lokale Jondo die Anfrage an einen zufällig ausgewählten Jondo seiner Gruppe, möglicherweise an sich selbst. Ein Jondo, der eine Anfrage von einem anderen Teilnehmer empfängt, leitet sie mit Wahrscheinlichkeit p_f wiederum an einen zufällig ausgewählten Jondo weiter, andernfalls an den Server. Die Antwort des Servers wird auf dem so ausgewählten Pfad in der umgekehrten Richtung zum Nutzer übertragen. Die Kommunikation zwischen dem ersten und dem letzten Jondo wird mit einem vom Initiator erzeugten Schlüssel verschlüsselt, der in jedem Schritt verschlüsselt weitergegeben wird, also allen Beteiligten bekannt ist. Die weitergeleiteten Nachrichten werden von den Jondos nicht umkodiert.

4.5.2 Sicherheit

Für den WWW-Anbieter ist jedes Mitglied der Crowd als Sender gleich wahrscheinlich. Die Wahrscheinlichkeit, daß er den Zugriff dem Nutzer A korrekt zuordnet, ist $\mathcal{G} = 1/n$, der Nutzer ist also *außer Verdacht.* Würde der lokale Jondo sich nicht selbst auswählen, wäre $\mathcal{G} = \frac{1}{n-1}$, was bei kleinen Crowds nachteilig wäre.

Ein Angreifer, der die Kommunikation des Nutzers abhört, kann zwar feststellen, daß der Nutzer einen WWW-Abruf durchführt; wer der Empfänger ist, erfährt er aber nicht, da die Kommunikation mit den folgenden Jondo verschlüsselt wird. Wenn der Jondo des Nutzers den Zugriff jedoch selbst durchführt, kann der Angreifer kann die unverschlüsselte Kommunikation mit dem Server beobachten. Zusätzlich erfährt er, daß der Jondo des Nutzers die Anfrage nicht von einem anderen Jondo erhalten hat und die Antwort nicht weiterleitet. Wenn der lokale Jondo sich, wie in [Reiter 1997], auch selbst auswählen kann, führt er den Zugriff mit Wahrscheinlichkeit $\frac{1-p_f}{n}$ selbst durch. Zusätzlich besteht die Möglichkeit, daß der zufällige Pfad im Jondo des Initiators endet. Dieser Fall ist für den Angreifer erkennbar, da die Nachrichten zwischen den Jondos nicht umkodiert werden.

In Bezug auf interne Angreifer ist der Abrufer *wahrscheinlich unbeteiligt,* wenn der Anteil ehrlicher Teilnehmer um einen von p_f abhängenden Faktor größer ist als der der kompromittierten [Reiter 1997]. Für den Angreifer ist es dann wahrscheinlicher, daß der Jondo die Anfrage von einem anderen ehrlichen Jondo erhalten hat, als daß es sich um eine Anfrage des lokalen Nutzers handelt.

Gegen einen Angreifer, der mit einem der beteiligten Jondos kooperiert und zusätzlich die Kommunikationsverbindung des Nutzers abhören kann, bietet das Verfahren keinen Schutz. Dieser Angreifer kann feststellen, daß der Nutzer den Zugriff selbst veranlaßt hat und, da er den verwendeten Schlüssel kennt, auch die Kommunikation zwischen Nutzer und Server entschlüsseln.

Ein Angreifer, der die Kommunikation des Nutzers und die Kommunikation zwischen dem letzten Jondo und dem Server abhören kann, kann die unverschlüsselten Daten anhand ihrer Länge und der Zugriffszeit den verschlüsselten zuordnen. Auch in diesem Fall ist die Anonymität des Nutzers somit nicht gewährleistet.

Kapitel 5

Kryptographisch sichere Anonymisierungsverfahren

5.1 Das ideale Modell

Im idealen Modell der anonymen Kommunikation existiert eine vertrauenswürdige Instanz, die Mitteilungen anonymisiert weiterleitet. Jeder Teilnehmer verfügt über einen sicheren Kanal zur vertrauenswürdigen Instanz. Die vertrauenswürdige Instanz gibt die Mitteilungen, die sie von den Teilnehmern erhält, anonymisiert weiter *(Sender-Anonymität);* Mitteilungen an anonyme Adressen stellt sie dem Empfänger zu *(Empfänger-Anonymität).* Da die Instanz vertrauenswürdig ist und die sicheren Kanäle nicht abgehört werden können, ist das Senden und Empfangen von Mitteilungen sowie die Beziehung von Sender und Empfänger unbeobachtbar. Somit erreicht dieses Verfahren perfekte Unbeobachtbarkeit und Anonymität. Die Anonymitätsmenge ist die Menge aller ehrlichen (nicht mit dem Angreifer kooperierenden) Teilnehmer.

Der Angreifer kennt im idealen Modell die Mitteilungen, die von den mit ihm kooperierenden Instanzen gesendet wurden. Er kann die Mitteilungen beobachten und ggf. beeinflussen, die an eine mit ihm kooperierende Instanz gesendet oder an alle Teilnehmer verteilt werden. Beobachtet der Angreifer eine ihm nicht bekannte Mitteilung, muß somit einer der ehrlichen Teilnehmer der Absender sein. Jede dem Angreifer nicht bekannte anonyme Adresse muß einem der ehrlichen Teilnehmer gehören. Es ist nicht geheim, wer an dem Verfahren teilnimmt. Je weniger ehrliche Teilnehmer es gibt, desto größer ist die Wahrscheinlichkeit, daß der Angreifer eine anonyme Mitteilung korrekt ihrem Absender zuordnet.

Ein reales Verfahren kann keine besseren Ergebnisse erzielen als das ideale [Micali 1992]; die Informationen, die der Angreifer im idealen Modell kennt, stehen ihm auch bei realen Verfahren zur Verfügung.

Ein reales Anonymisierungsverfahren ist sicher, wenn es das ideale Modell mit kryptographischen Methoden so simuliert, daß ein Angreifer keine zusätzlichen Informationen gewinnen kann, obwohl keine physikalisch gesicherten Kanäle zur Verfügung stehen und keine einzelne Instanz als vertrauenswürdig feststeht [Beaver 1992, Goldreich 1997].

Indem die Kommunikation zwischen zwei Instanzen so verschlüsselt wird, daß der Angreifer aus den abgehörten Nachrichten keine Informationen gewinnen kann, wird ein sicherer Kanal simuliert. Wenn die Länge der verschlüsselten Nachrichten erkennbar bleibt, müssen zusätzlich bedeutungslose Nachrichten übertragen werden, um dem Angreifer keine Informationen darüber zu geben, ob Kommunikation stattfindet.

Eine vertrauenswürdige Instanz kann simuliert werden, indem mehrere Instanzen zusammenarbeiten, von denen zumindest ein Teil in Bezug auf eine bestimmte Funktion vertrauenswürdig ist. Welche Instanzen tatsächlich die ehrlichen sind, muß dabei nicht bekannt sein.

In realen Verfahren muß der Sender alle Nachrichten zusätzlich zu der in Anonymisierungsverfahren eingesetzten Verschlüsselung mit einem Schlüssel des Empfängers verschlüsseln, um die Vertraulichkeit der Inhaltsdaten sicherzustellen (Ende-zu-Ende-Verschlüsselung).

5.2 Kryptographie

Kryptographische Verfahren dienen dem Schutz von Daten vor Fälschung, Veränderung und unbefugter Kenntnisnahme.

5.2.1 Verschlüsselung

Ein Kryptosystem besteht aus [Menezes 1997]:

- einem Klartextraum $\mathcal{M}$,
- einem Geheimtextraum $\mathcal{C}$,
- einem Schlüsselraum $\mathcal{K}$,
- einer Menge $\{E_e\colon\ e \in \mathcal{K}\}$ von Verschlüsselungsfunktionen $E_e\colon\ \mathcal{M} \to \mathcal{E}$ (bei *probabilistischen* Kryptosystemen ist E_e statt dessen ein nichtdeterministischer Algorithmus),
- einer korrespondierenden Menge $\{D_d\colon\ d \in \mathcal{K}\}$ von Entschlüsselungsfunktionen $D_d\colon\ \mathcal{C} \to \mathcal{M}$ mit der Eigenschaft, daß es zu jedem $e \in \mathcal{K}$ einen Schlüssel d gibt, so daß $D_d(E_e(m)) = m$ für alle $m \in \mathcal{M}$.

$\mathcal{M}, \mathcal{C}, \mathcal{K}, \{E_e\}$ und $\{D_d\}$ müssen nicht geheimgehalten werden.

Wenn es innerhalb einer angemessenen Zeitspanne möglich ist, ohne Kenntnis des Schlüssels d aus einem Geheimtext systematisch Informationen – neben der Tatsache, daß ein Text der gegebenen Länge vorliegt – über den entsprechenden Klartext zurückzugewinnen, ist ein Kryptosystem *unsicher*.

5.2.2 Sicherheit

Angriffe auf ein Kryptosystem werden danach unterschieden, ob der Angreifer nur Geheimtexte beobachtet *(ciphertext-only attack),* Paare von Klartexten und zugehörigen Geheimtexten kennt *(known-plaintext attack),* Klartexte selbst auswählen kann und die zugehörigen Geheimtexte erhält *(chosen-plaintext attack)* oder Geheimtexte auswählen kann und die entsprechenden Klartexte erhält *(chosen-ciphertext attack).* Gegen letzteren Angriff muß das Kryptosystem sicher sein, wenn der Angreifer wie beim Mix-Netz (siehe Kapitel 6) beliebige Geheimtexte entschlüsseln lassen kann.

Ein Kryptosystem ist **informationstheoretisch** oder **perfekt sicher** [Menezes 1997], wenn für einen Angreifer mit unbegrenzter Rechenkapazität bei Kenntnis des Geheimtextes alle denkbaren Klartexte gleich wahrscheinlich sind, wenn der Geheimtext dem Angreifer also, von der Länge abgesehen, keine Informationen über den Klartext gibt. Perfekte Sicherheit ist nur möglich, wenn der Schlüssel mindestens so lang ist wie die (eventuell vorher komprimierte) zu übertragende Nachricht. Durch das daraus resultierende Schlüsselverteilungsproblem werden perfekt sichere Verfahren für die Anwendung in offenen Netzen unpraktikabel. Asymmetrische Verschlüsselungsverfahren (Abschnitt 5.2.4) können nicht perfekt sicher sein, da ein in der Rechenzeit nicht beschränkter Angreifer mit Kenntnis des öffentlichen Schlüssels sämtliche möglichen Verschlüsselungen durchführen kann, bis er den gegebenen Geheimtext erhält.

Eine obere Grenze für den Aufwand zum Brechen jedes nicht perfekt sicheren Kryptosystems ist durch die Größe des Schlüsselraumes gegeben. Ein Angreifer kann den Geheimtext systematisch mit allen $k \in \mathcal{K}$ zu entschlüsseln versuchen, bis er den Klartext erhält. $\mathcal{K}$ muß daher so groß gewählt werden, daß dieser Angriff innerhalb absehbarer Zeit nicht durchgeführt werden kann.

Gibt der Geheimtext einem auf effiziente Berechnungen beschränkten Angreifer abgesehen von einer oberen Schranke für die Länge der Nachricht keine Informationen über den Klartext, ist das Kryptosystem **semantisch sicher.** Dieses Modell beruht auf der Annahme, daß bestimmte Berechnungen nicht praktikabel sind. Ein Kryptosystem heißt **kryptographisch sicher,** wenn gezeigt werden kann, daß das Brechen des Systems so schwer ist, wie die Lösung eines wohlbekannten und als schwierig angesehen Problems zu finden.

5.2.3 Symmetrische Verschlüsselung

In einem **symmetrischen** Kryptosystem kann d einfach aus e bestimmt werden. Üblicherweise ist dann $e = d$. Dieser **geheime Schlüssel** muß vorab über einen sicheren Kanal ausgetauscht werden.

Blockchiffren sind symmetrische Kryptosysteme, bei dem der Klartext in Blöcke einer festen Länge unterteilt und jeweils ein Block zur Zeit verschlüsselt wird. Blockchiffren können in verschiedenen Betriebsmodi verwendet werden. Im ECB-Modus wird jeder Block unabhängig von den anderen verschlüsselt; identische Klartextblöcke ergeben daher identische Geheimtextblöcke. Datenmuster bleiben daher im Geheimtext erkennbar; ein Angreifer kann unbemerkt Blöcke vertauschen oder einfügen. Für Nachrichten, die länger als die Blockgröße sind, ist dieser Modus somit unsicher. In anderen Modi werden vorhergehende Blöcke in die Verschlüsselungsoperation einbezogen.

Symmetrische Verfahren wie Triple-DES und IDEA in geeigneten Modi werden allgemein als sicher angesehen, da trotz ausführlicher Analyse keine Möglichkeit gefunden wurde, sie zu brechen.

In kryptographischen Protokollen werden häufig zufällige Daten benötigt. **Pseudozufallsgeneratoren** wählen mit Hilfe eines geheimgehaltenen *Initialisierungswertes (seed)* eine Folge von Elementen aus einer Menge M aus, wobei es für einen Angreifer ohne Kenntnis des Initialisierungswertes nicht praktikabel ist, sie von gleichverteilt gewählten zu unterscheiden. Notiert wird die pseudozufällige Auswahl eines Elements x als $x \in_R M$. Werden zu verschlüsselnde Daten mit Pseudozufallsdaten bitweise *exklusiv-oder*-verknüpft, ensteht eine *Stromchiffre,* deren geheimer Schlüssel der Initialisierungswert ist.

5.2.4 Asymmetrische Verschlüsselung

Ein Kryptosystem heißt **asymmetrisch,** wenn es auch dann sicher ist, wenn der Angreifer E_e kennt. e kann daher veröffentlicht werden und heißt auch **öffentlicher Schlüssel**; d ist der **private Schlüssel.**

Asymmetrische Kryptosysteme beruhen auf *Einwegfunktionen mit Falltür.* Eine **Einwegfunktion** ist eine effizient berechenbare Funktion, deren Umkehrung sich nur mit vernachlässigbarer Wahrscheinlichkeit effizient berechnen läßt; bei einer Einwegfunktion mit Falltür ist die Umkehrung nur mit Kenntnis eines geheimen Parameters *(Falltürinformation)* effizient zu berechnen. Ob es Einwegfunktionen wirklich gibt, ist nicht bekannt. Funktionen, von denen angenommen wird, daß sie diese Eigenschaft erfüllen, beruhen beispielsweise auf der Schwierigkeit, Zahlen in ihre Primfaktoren zu zerlegen oder diskrete Logarithmen zu berechnen. Die Algorithmen RSA und ElGamal werden bei Verwendung von Schlüssellängen ab 1024 Bit als sicher angesehen; für auf elliptischen Kurven basierende Verfahren gelten kürzere Schlüssel als sicher.

Ein *probabilistischer* Verschlüsselungsalgorithmus wählt zufällig einen von verschiedenen möglichen Geheimtexten aus. Die Menge der möglichen Geheimtexte muß so groß sein, daß es nicht praktikabel ist, alle Verschlüsselungen eines Klartextes systematisch auszuprobieren, um die Zuordnung zu finden. Semantisch sichere asymmetrische Kryptosysteme müssen probabilistisch sein, da ein Angreifer sonst beliebige Klartexte mit dem öffentlichen Schlüssel des Empfängers verschlüsseln und den resultierenden Geheimtext mit dem ihm vorliegenden vergleichen kann [Goldreich 1997]. Die Entschlüsselung von Nachrichten aus einem kleinen, bekannten Klartextraum ist bei deterministischen asymmetrischen Kryptosystemen trivial [Bellare 1997].

Ein Kryptosystem heißt *plaintext aware,* wenn es ohne Kenntnis des Klartextes nicht praktikabel ist, einen gültigen Geheimtext zu erzeugen. Dies läßt sich erreichen, indem der Klartext Redundanz enthält, die beim Entschlüsseln geprüft wird. Bei anderen Kryptosystemen besteht die Möglichkeit, daß ein Angreifer Geheimtexte durch adaptive *chosen-ciphertext*-Angriffe entschlüsseln kann.

Aktive Angriffe auf die asymmetrische Verschlüsselung nach PKCS #1 [RSA 1993] sind nicht bekannt [Bellare 1997]. Die Sicherheit von OAEP [Bellare 1995] ist bewiesen unter der Annahme, daß ideale Hash-Funktionen existieren *(random-oracle*-Modell). Diese Verfahren können auf RSA aufgesetzt werden.

Der Aufwand für asymmetrische Ver- und Entschlüsselung ist i. a. höher als der für symmetrische. Asymmetrische Verfahren werden in der Praxis mit symmetrischen zu *Hybridverfahren* kombiniert, indem nur ein zufällig gewählter Sitzungsschlüssel für das symmetrische Verfahren asymmetrisch verschlüsselt wird.

5.2.5 Forward secrecy

Zusätzlich ist es wünschenswert, daß ein Angreifer im Nachhinein selbst dann keine Informationen über in der Vergangenheit übertragene Nachrichten gewinnen kann, wenn einer der dauerhaften privaten Schlüssel zu einem späteren Zeitpunkt kompromittiert wird. Diese als *forward secrecy* bezeichnete Eigenschaft eines Kryptosystems kann durch ein Protokoll zum Vereinbaren geheimer Sitzungsschlüssel wie Diffie-Hellman erreicht werden [Goldwasser 1997]. An Anonymisierungsdienste ergibt sich daraus die zusätzliche Anforderung, daß keine Log-Dateien geführt werden sollten, die über die Identität der Nutzer Auskunft geben [Goldberg 1997].

5.2.6 Authentizität

Eine *Hash-Funktion* ist eine effizient berechenbare Funktion, die Zeichenketten beliebiger Länge auf Zeichenketten einer festen Länge („Hash-Werte") abbildet. Wenn es nicht praktikabel ist, für eine Hash-Funktion h zwei Eingaben x und y zu finden, so daß $h(x) = h(y)$ gilt *(Kollisionsresistenz)*, oder zu einem gegebenen Hash-Wert y ein x mit $dpph(x) = y$ zu finden, ist h eine **kryptographische Hash-Funktion.**

Ein *Message Authentication Code* (MAC) ist eine schlüsselabhängige Hash-Funktion. Der Sender einer Nachricht x berechnet $h_k(x)$ für einen ihm und dem Empfänger bekannten geheimen Schlüssel k und überträgt $(x, h_k(x))$. Der Empfänger berechnet ebenfalls $h_k(x)$. Wenn die Werte übereinstimmen, ist die Nachricht authentisch, da ein Angreifer ohne Kenntnis von k keinen gültigen MAC bilden kann.

Digitale Signaturen gewährleisten ebenfalls die Authentizität und ermöglichen dem Empfänger zusätzlich, gegenüber einem Dritten zu beweisen, daß der Sender die Nachricht signiert hat. Der Sender kann mit seinem privaten Schlüssel d und der Signierfunktion $S_d\colon\ \mathcal{M} \to \mathcal{C}$ (oder einem nichtdeterministischen Signieralgorithmus S_d) Signaturen für seine Nachrichten generieren. Mit dem zu d gehörigen öffentlichen Schlüssel e und der Verifikationsfunktion $V_e\colon\ \mathcal{M} \times \mathcal{C} \to \{\mathsf{wahr}, \mathsf{falsch}\}$ kann der Empfänger die Authentizität der signierten Nachricht prüfen. Signaturverfahren können aus asymmetrischen Kryptosystemen, meist in Verbindung mit einer Hash-Funktion, konstruiert werden.

5.2.7 Zero-Knowledge-Beweise

Ein **Zero-Knowledge-Beweissystem** ist ein Protokoll, das es einem Beweiser A erlaubt, einen Verifizierer B von der Gültigkeit einer Behauptung zu überzeugen, ohne irgendwelche weiteren Informationen über sie preiszugeben. Wenn eine Instanz über ein Geheimnis verfügt und abhängig von diesem Geheimnis handeln soll, kann sie einen Zero-Knowledge-Beweis verwenden, um zu zeigen, daß sie korrekt gehandelt hat, ohne ihr Geheimnis preiszugeben [Goldreich 1997].

In einem *interaktiven Beweissystem* tauschen Verifizierer und Beweiser Nachrichten *(challenge, response)* aus. Ein ehrlicher Beweiser sollte einen ehrlichen Verifizierer mit überwältigender Wahrscheinlichkeit davon überzeugen können, daß er das Geheimnis kennt *(completeness);* ein unehrlicher Beweiser sollte das Protokoll ohne Kenntnis des Geheimnisses nur mit vernachlässigbarer Wahrscheinlichkeit erfolgreich durchführen können *(soundness).*

Das Beweissystem hat die *zero-knowledge*-Eigenschaft, wenn es einen Algorithmus polynomieller Laufzeit *(Simulator)* gibt, der mit der Eingabe der zu beweisenden Eigenschaft ohne Interaktion mit dem Beweiser eine Ausgabe erzeugen kann, die vom Transkript einer Interaktion mit dem Beweiser nicht zu unterscheiden ist. Aus dieser Eigenschaft folgt, daß das Protokoll – auch bei Interaktion mit einem aktiven Angreifer als Verifizierer – außer der Gültigkeit der Behauptung keine Informationen über das Geheimnis preisgibt [Menezes 1997].

Aus einem interaktiven Zero-Knowledge-Beweis läßt sich ein nicht-interaktiver erzeugen, indem die Rolle des Verifizierers durch eine kryptographische Hash-Funktion ersetzt wird [Schneier 1996].

5.3 Konsistente Verteilung

Zum Schutz des Empfängers können die Nachrichten an eine große Zahl potentieller Empfänger verteilt werden *(broadcast).* Ein Angreifer, der alle Kommunikationsverbindungen abhört und mit einem Teil der Teilnehmer kooperiert, erhält dann aus seinen Beobachtungen keinerlei Informationen darüber, an wen die Nachricht gerichtet ist und ob sie überhaupt einen Empfänger hat. Durch Verteilung läßt sich somit perfekte Empfänger-Anonymität erreichen [Pfitzmann 1990].

Sofern der Empfänger auf empfangene Nachrichten reagiert, kann ein aktiver Angreifer ihn jedoch identifizieren, indem er die Konsistenz der Verteilung stört (Abschnitt 3.6). Somit muß sichergestellt werden, daß die Verteilung konsistent erfolgt.

Werden Nachrichten verteilt, die für einzelne Empfänger bestimmt sind, muß der Empfänger die an ihn gerichteten Nachrichten anhand einer **impliziten Adresse** erkennen können. Ist die Adresse nur für den Empfänger erkennbar, spricht man von *verdeckter Adressierung*. Erreichen läßt sich dies durch asymmetrische Verschlüsselung, indem der Empfänger versucht, alle Nachrichten mit den zu seinen Pseudonymen gehörenden Schlüsseln zu entschlüsseln. Eine korrekte Entschlüsselung ist durch im Klartext enthaltene Redundanz erkennbar. Um zu vermeiden, daß eine große Zahl von Entschlüsselungsoperationen notwendig wird, kann als *offene Adressierung* ein für jeden erkennbares Merkmal verwendet werden. Nachrichten mit derselben offenen Adresse sind verkettbar [Pfitzmann 1990].

5.3.1 Anwendung im Internet

Usenet-Newsgroups [Horton 1987] sind ein – nicht zuverlässiges – Verteil-Medium. Für den anonymen Empfang von Nachrichten wurde die Newsgroup `alt.anonymous.messages` eingerichtet. Um anonym zu bleiben, muß ein Nutzer alle in der Newsgroup vorhandenen Nachrichten vom News-Server abrufen, da der Zugriff für den Betreiber des Servers beobachtbar ist, und die an ihn gerichteten Nachrichten *lokal auswählen.* Im Usenet ist es leicht möglich, Nachrichten zu unterdrücken: Die Steueranweisungen `cancel` und `Supersedes` dienen zum Löschen von Nachrichten; durch Manipulation des `Path`-Headers[1] oder durch Erzeugen weiterer Nachrichten mit derselben `Message-ID` läßt sich die Verteilung einer Nachricht unter Umständen gezielt einschränken.

5.3.2 Sicherstellung der Konsistenz

Werden die Nachrichten vor der Verteilung mit Sequenznummern versehen und von einer vertrauenswürdigen oder mehreren unabhängigen Instanzen signiert [Pfitzmann 1990], können die Empfänger das Fehlen einzelner Nachrichten entdecken und sie über einen anderen Kanal abrufen; Angriffe lassen sich so aber nicht von im Netz aufgetretenen Fehlern unterscheiden.

Um eine zuverlässige Verteilung zu erreichen, muß jeder Teilnehmer als *Rückmeldung* einen signierten Hash-Wert der empfangenen Nachrichten an alle anderen verteilen [Pfitzmann 1989]. Solange Signaturen fehlen oder falls Hash-Werte nicht übereinstimmen, darf der anonyme Empfänger die Nachricht nicht beantworten. Durch dieses Verfahren gewinnt der Angreifer keinerlei Informationen über den Empfänger der Nachricht, es ist jedoch mit großem Aufwand verbunden: Jeder Teilnehmer erhält sämtliche Nachrichten, die für die Mitglieder seiner Anonymitätsmenge bestimmt sind und zusätzlich signierte Hash-Werte von jedem Teilnehmer.

5.4 Das DC-Netz

Das nach dem von D. Chaum diskutierten Problem der *dining cryptographers* benannte DC-Netz [Chaum 1988] erreicht perfekte Unbeobachtbarkeit und Anonymität des Senders durch **überlagerndes Senden.** Das DC-Protokoll wird in *Runden* ausgeführt. In jeder Runde senden alle Teilnehmer. Durch Überlagerung der Nachrichten ergibt sich ein unbeobachtbarer *Mehrfachzugriffskanal* [Waidner 1990].

[1] Der `Path`-Header sagt aus, daß die betreffende Nachricht bei den dort angegebenen Systemen bereits vorliegt. Bestimmte Optimierungen der Verteilung können dazu führen, daß dort fälschlich eingetragene Systeme die Nachricht gar nicht erhalten.

5.4.1 Überlagerndes Senden

Ein DC-Netz besteht aus einer festen Menge von Teilnehmern $\{\mathsf{T}_1, \mathsf{T}_2, \ldots, \mathsf{T}_n\}$ und setzt voraus, daß eine endliche abelsche Gruppe $(G, +)$ festgelegt wurde. Die Menge G ist das *Alphabet* des DC-Netzes.

Vor Beginn der Übertragung vereinbaren alle Paare von Teilnehmern $\mathsf{T}_i, \mathsf{T}_j$ jeweils für jede Runde r einen gemeinsamen geheimen Schlüssel $K^r_{i,j} = K^r_{j,i} \in_R G$. Werden diese Schlüssel zufällig gewählt und über einen sicheren Kanal ausgetauscht, ist das DC-Netz *informationstheoretisch sicher.* Wenn die Teilnehmer mittels eines asymmetrischen Kryptosystems einen Initialisierungswert für einen kryptographischen Zufallsgenerator austauschen, ist das Verfahren *kryptographisch sicher.* Wenn zwei Teilnehmer $\mathsf{T}_i, \mathsf{T}_j$ sich gegenseitig nicht vertrauen, brauchen sie keinen Schlüssel zu vereinbaren. Dann sei $K_{i,j} := 0$.

Jeder Teilnehmer T_i wählt für jede Runde r seine Nachricht $N_i \in G$ und bildet seine **lokale Ausgabe:**

$$O^r_i := N^r_i + \sum_{j=1}^{i-1} K^r_{i,j} - \sum_{j=i+1}^{n} K^r_{i,j} \tag{5.1}$$

[Lukat 1991].

Aus den lokalen Ausgaben wird die **globale Summe**

$$S^r := \sum_{i=1}^{n} O^r_i = \sum_{i=1}^{n} \left(N^r_i + \sum_{j=1}^{i-1} K^r_{i,j} - \sum_{j=i+1}^{n} K^r_{i,j} \right) = \sum_{i=1}^{n} N^r_i \tag{5.2}$$

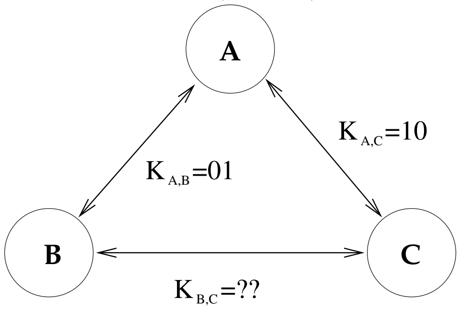
gebildet und verteilt. Hat in einer Runde genau ein Teilnehmer eine Nachricht $N^r_i \neq 0$ gewählt, wird somit N^r_i an alle Teilnehmer verteilt, d. h. es erfolgte dann eine *kollisionsfreie* Übertragung.

5.4.2 Sicherheit

Eine externer Angreifer hat keine Informationen über die Schlüssel $K_{i,j} \in G$ und kann demzufolge den beobachteten O_i keine Informationen über die Nachrichten N_i entnehmen.

Ein interner Angreifer kennt einen Teil der Schlüssel. Um die resultierende Sicherheit des DC-Netzes zu untersuchen, wird der **Schlüsselgraph** des DC-Netzes $G := (\{\mathsf{T}_1, \mathsf{T}_2, \ldots, \mathsf{T}_n\}, \{\mathsf{T}_i \times \mathsf{T}_j \colon\ i, j \in \{1, 2, \ldots, n\}, i \neq j, K_{i,j} \text{ wurde ausgetauscht}\})$ betrachtet. Aus diesem Graphen werden die Kanten entfernt, die dem Angreifer bekannte Schlüssel darstellen. Innerhalb der zusammenhängenden Komponenten des resultierenden Graphen kann der Angreifer nur Summe der Nachrichten aller Teilnehmer feststellen und keine Informationen über einzelne Teilnehmer gewinnen. Sie stellen somit die resultierenden Anonymitätsmengen dar. Ist der Schlüsselgraph zusammenhängend, ist das DC-Netz also perfekt sicher.

$$O_{\mathsf{A}} := N_{\mathsf{A}} + K_{\mathsf{A,B}} + K_{\mathsf{A,C}} = 00 + 01 + 10 = 11$$



$$\begin{array}{ll} O_{\mathsf{A}} & = 11 \\ O_{\mathsf{B}} & = 10 \\ O_{\mathsf{C}} & = 01 \\ \hline S & = 01 \end{array}$$

A weiß, daß $N_{\mathsf{B}} + N_{\mathsf{C}} = 01$, hat aber keine weiteren Informationen über N_{B} und N_{C}.

Abbildung 5.1: Anonymität im DC-Netz (Beispiel)

Für jeden Vektor $(N_1, \ldots, N_n)$ der Nachrichten, der mit dem anfänglichen Wissen des Angreifers über die Nachrichten konsistent ist und $\sum_{j=1}^{n} N_j = \sum_{j=1}^{n} O_j$ für die beobachteten lokalen Ausgaben $(O_1, \ldots, O_n)$ erfüllt, existiert die gleiche Anzahl von Schlüsselkombinationen, die (5.1) erfüllen [Waidner 1990]. Daher ist die bedingte Wahrscheinlichkeit für $(N_1, \ldots, N_n)$ bei gegebenen $(O_1, \ldots, O_n)$ gleich der bedingten Wahrscheinlichkeit für $(N_1, \ldots, N_n)$, wenn nur die Summe aller Nachrichten gegeben ist. Somit erhält der Angreifer bei bezüglich der Schlüssel zusammenhängenden Teilnehmern und Ende-zu-Ende-Verschlüsselung der Nachrichten genau die Informationen über die Nachrichten der Teilnehmer, über die er im idealen Modell verfügt.

Entsprechendes gilt für aktive Angriffe auf die Sender-Anonymität: Unter der Voraussetzung, daß er mindestens einen der Schlüssel des angegriffenen Teilnehmers nicht kennt, kann ein Nachrichten unterdrückender oder verändernder Angreifer anhand seiner Beobachtungen nicht unterscheiden, ob der Teilnehmer eine Mitteilung gesendet hat oder nicht. Werden Nachrichten unterdrückt oder durch unabhängig von den beobachteten gewählte Nachrichten ersetzt, ist die globale Summe unlesbar. Wenn der Angreifer zu den beobachteten Nachrichten etwas addiert, ändert sich die globale Summe entsprechend; auch dadurch werden keine Rückschlüsse auf einzelne Teilnehmer möglich.

Empfänger-Anonymität muß im DC-Netz durch konsistente Verteilung gewährleistet werden.

5.4.3 fail-stop-Schlüsselerzeugung

Die Empfänger-Anonymität kann durch Rückmeldungen aller Teilnehmer gewährleistet werden. Eine effizientere Möglichkeit besteht darin, die globale Summe vorausgegangener Runden so in die Schlüsselerzeugung des überlagernden Sendens einzubeziehen, daß die Übertragung im Fall einer inkonsistenten Verteilung gestört wird *(fail-stop-Schlüsselerzeugung)*. Dieses Verfahren wird als **DC$^+$-Netz** bezeichnet [Waidner 1990].

Solange die lokalen Eingaben I_i, I_j zweier Teilnehmer $\mathsf{T}_i, \mathsf{T}_j$ identisch sind, sollen sie denselben pseudozufällig gewählten Schlüssel $K_{i,j} = K_{j,i}$ verwenden:

$$\left[\forall r < r' \colon\ I_i^r = I_j^r\right] \Rightarrow K_{i,j}^{r'} = K_{j,i}^{r'} \in_R G \tag{5.3}$$

Wenn T_i und T_j in einer Runde unterschiedliche lokale Eingaben erhalten, sollen ihre Schlüssel in den folgenden Runden unabhängig voneinander sein, so daß die resultierende globale Summe von den gesendeten Nachrichten unabhängig ist:

$$\left[\exists r < r' \colon\ I_i^r \neq I_j^r\right] \Rightarrow K_{i,j}^{r'} \in_R G, K_{j,i}^{r'} \in_R G \tag{5.4}$$

Die Schlüsselerzeugung muß also vollständig, aber nicht ausschließlich von den bereits empfangenen Zeichen abhängen. Um (5.4) deterministisch erfüllen zu können, müssen die Teilnehmer somit zwischen allen denkbaren Eingabesequenzen unterscheiden können und daher alle bereits empfangenen Zeichen speichern [Waidner 1990].

Eine effizientere Lösung ist für eine probabilistische Variante von (5.4) möglich:

$$\left[I_i^{r_0} \neq I_j^{r_0} \wedge \forall r < r_0 \colon\ I_i^r = I_j^r\right] \Rightarrow \forall r' \in \{r_0, \dots, r_0 + d\} \colon\ K_{i,j}^{r'} \in_R G, K_{j,i}^{r'} \in_R G \tag{5.5}$$

Wenn also in der Runde r_0 erstmals eine Inkonsistenz auftritt, stören T_i und T_j das überlagernde Senden für d Runden. Das maximale d, für das (5.5) erfüllt ist, ist eine Zufallsvariable mit einem Wahrscheinlichkeitsmaß $\mathrm{P}(d)$.

Seien G ein endlicher Körper, $(a_1, a_2, \dots), (b_3, b_4, \dots) \in_R G^{\mathbb{N}}, c \in_R G$ geheime zwischen T_i und T_j vereinbarte Werte, $b_1, b_2, K^0, I^0 := 0$. Dann sei

$$K^r := a_r + (c + K^{r-1})(b_r + I^{r-1}). \tag{5.6}$$

Dieses Verfahren erfüllt (5.3) und (5.5) mit

$$\mathrm{P}(d) = \frac{1}{|G|}\left(1 - \frac{1}{|G|}\right)^{d-1}.$$

Für die Wahrscheinlichkeit eines erfolgreichen Angriffs in $r_{\max}$ Runden gilt: $\mathrm{P}_A \leq \frac{r_{\max}}{|G|}$ [Lukat 1991]. Eine sinnvolle Elementanzahl des verwendeten Körpers wäre z. B. $|G| = 2^{108}$ [Waidner 1990].

Die durch die Schlüsselerzeugung verursachte Verzögerung kann reduziert werden, indem sie für mehrere Runden parallel durchgeführt wird. Das DC$^+$-Protokoll kann in einer Zeitscheibentechnik in mehreren Slots unabhängig voneinander ausgeführt werden, wobei alle zusammenhängenden Interaktionen dann in demselben DC^+-Netz durchgeführt werden sollten, um die Unbeobachtbarkeit nicht zu gefährden. Eine andere Möglichkeit besteht darin, die Schlüssel nicht abhängig von der unmittelbar vorhergehenden Runde zu erzeugen, sondern nur diejenigen zu berücksichtigen, die in einem bestimmten Abstand vor der aktuellen Runde liegen. Die Teilnehmer müssen dann entsprechend lange warten, bis sie auf eine empfangene Nachricht reagieren, um ihre Unbeobachtbarkeit zu erhalten [Waidner 1990].

5.4.4 Mehrfachzugriff auf den unbeobachtbaren Kanal

Der Zugriff auf den Kanal muß durch ein Protokoll geregelt werden, das die Unbeobachtbarkeit der Sender erhält. Außerhalb dieses Kanals können die Teilnehmer nicht unbeobachtbar kommunizieren. Da es sich um einen Verteil-Kanal handelt, auf den alle Teilnehmer lesend und schreibend zugreifen können, können verschiedene für die Mediumzugriffssteuerung entwickelte Protokolle [Tanenbaum 1989] eingesetzt werden.

Die Sender können Kollisionen erkennen $(S^r \neq N_i)$. Wenn die Teilnehmer die Nachrichten aus dem Alphabet $G \setminus \{0\}$ wählen, kann jeder Teilnehmer feststellen, ob der Kanal belegt ist $(S^r \neq 0)$.[2]

Die zu übertragenden Daten werden in Nachrichten fester Länge (Rahmen) eingeteilt, die aus einer oder aus mehreren aufeinander folgenden Runden des überlagernden Sendens von Zeichen aus G bestehen. Jede Nachricht muß eine implizite Adressierung enthalten, damit der Empfänger erkennen kann, daß sie an ihn gerichtet ist.

Die Effizienz eines Protokolls hängt zum einen vom erzielten Durchsatz ab, zum anderen von der von ihm verursachten Verzögerung. Der Durchsatz sinkt, wenn Kollisionen auftreten und wenn niemand sendet, obwohl sendewillige Teilnehmer vorhanden sind.

5.4.4.1 Contentionverfahren

Das einfachste Verfahren, **ALOHA,** erlaubt es den Teilnehmern, immer zu senden, wenn sie eine Nachricht übertragen wollen. Wenn eine dabei Kollision auftritt, überträgt der Sender die gestörte Nachricht nach einer zufällig gewählten Wartezeit noch einmal. Bei der wiederholten Übertragung muß die Nachricht anders Ende-zu-Ende-verschlüsselt werden. Andernfalls könnte ein Angreifer schließen, daß Nachrichten, deren Summe eine Kollision ergeben hat, nicht von demselben Teilnehmer gesendet wurden, oder Teilnehmer würden die Übertragungskapazität des Netzes verschwenden, indem sie scheinbare Kollisionen ihrer eigenen Nachrichten übertragen [Pfitzmann 1990]. Die Wartezeit muß zufällig sein, damit zwei Teilnehmer sich nicht dauerhaft gegenseitig blockieren [Tanenbaum 1989].

[2] Daß sich beim Auftreten einer Kollision zufällig $S^r = 0$ ergeben kann, verursacht keine Probleme, wenn alle Teilnehmer diese Situation so behandeln, als ob der Kanal frei wäre.

Bei **Slotted ALOHA** wird der Kanal in Abschnitte *(Slots)* von der Länge eines Rahmens unterteilt; die Teilnehmer dürfen nur am Anfang eines Slots anfangen zu senden. Damit wird vermieden, daß der Anfang eines Rahmens mit dem Ende eines fast vollständig übertragenen kollidiert.

Bei einer geringen Anzahl sendewilliger Teilnehmer ist der Durchsatz sehr gut, bei höherer Last nimmt er schnell ab. Der maximale Durchsatz bei Slotted ALOHA beträgt $1/e \approx 37\,\%$ [Tanenbaum 1989].

Eine bessere Ausnutzung des Kanals als bei ALOHA ist möglich, wenn die Teilnehmer überprüfen, ob der Kanal belegt ist **(carrier sense protocols).** Im *p-persistenten CSMA*-Protokoll *(carrier sense multiple access)* wartet ein sendewilliger Teilnehmer, bis der Kanal frei ist. Dann sendet er mit Wahrscheinlichkeit p seine Nachricht; falls beim Senden der Nachricht eine Kollision auftritt, beginnt er nach einer zufälligen Wartezeit von vorne. Mit Wahrscheinlichkeit $q := 1 - p$ sendet er dagegen nicht sofort. Sofern im folgenden Zeitabschnitt noch kein anderer Teilnehmer begonnen hat zu senden, beginnt er seine Übertragung wiederum mit Wahrscheinlichkeit p und wartet mit Wahrscheinlichkeit q für einen weiteren Zeitabschnitt. Dies wiederholt er solange, bis die Nachricht übertragen ist [Tanenbaum 1989].

Da kein Teilnehmer eine Übertragung beginnt, während ein anderer sendet, treten weniger Kollisionen auf als bei Slotted ALOHA. Wenn während einer Übertragung mehrere Teilnehmer sendebereit werden, treten bei 1-persistentem CSMA Kollisionen auf, da die Teilnehmer nach dem Ende der Übertragung gleichzeitig anfangen zu senden. Bei hoher Last nutzt *p-persistentes CSMA* mit kleinem p den Kanal besser aus, bei niedriger Last verursacht es stärkere Verzögerungen. Nachrichten, die ein Sender nacheinander überträgt, ohne den Kanal zwischenzeitlich freizugeben, sind verkettbar [Pfitzmann 1990].

Eine weitere Optimierung besteht darin, die Übertragung einer Nachricht beim Auftreten einer Kollision sofort abzubrechen *(CSMA/CD, carrier sense multiple access with collision detection).* Die beteiligten Sender stellen beim Senden des ersten Zeichens fest, daß $S^1 \neq N_i$. In der folgenden Runde senden sie nicht mehr, so daß $S^2 = 0$. Daran können alle Teilnehmer erkennen, daß die Übertragung abgebrochen wurde und ab Runde 3 wieder nach zufälliger Verzögerung mit dem Senden einer Nachricht beginnen. Die Ausnutzung des Kanals wird somit verbessert.

CSMA und CSMA/CD erfordern, daß die Teilnehmer das Ergebnis des Sendens schnell erfahren. Wenn das DC-Netz eine eine große Verzögerungszeit hat, kann der anonyme Kanal in Slots unterteilt werden, in denen das Protokoll jeweils unabhängig ausgeführt wird.

5.4.4.2 Reservierungsverfahren

Bei starker Auslastung des Kanals ist es sinnvoll, Kollisionen durch den Einsatz eines Reservierungsverfahrens zu vermeiden. Protokolle, die darauf beruhen, daß jedem Teilnehmer ein eindeutiges Merkmal zugeordnet ist, können hierfür jedoch nicht eingesetzt werden, weil Sender-Anonymität erreicht werden soll.

In einem einfachen Reservierungsprotokoll enthält bei n Teilnehmern jede Gruppe von Slots einen speziellen Reservierungsslot mit r Zeichen aus $G := \mathbb{Z}/m\mathbb{Z}$ mit $m > n$ [Waidner 1990]. Ein sendewilliger Teilnehmer wählt zufällig ein $k \in_R \{1, \ldots, r\}$ und sendet als k-tes Zeichen eine 1. Eine 0 im Reservierungsslot bezeichnet einen nicht reservierten Slot, eine 1 eine erfolgreiche Reservierung; Zeichen aus $\{2, \ldots, m\}$ bezeichnen Kollisionen. Die Teilnehmer, bei deren Reservierung keine Kollision aufgetreten ist, senden dann in der Reihenfolge der von ihnen gewählten Zahlen k; Slots, für die sich bei der Reservierung ein von 1 verschiedenes Zeichen ergeben hat, werden ausgelassen. Wenn r groß gewählt wird, ist die Wahrscheinlichkeit einer Kollision gering. Eine obere Schranke für die Verzögerungszeit einer Nachricht kann aber auch bei diesem Verfahren nicht angegeben werden.

5.4.4.3 Kollisionsauflösung

Da Überlagerungs-Kollisionen anders als Kollisionen in einem analogen Kanal einen wohldefinierten Wert, die Summe der Zeichen, ergeben, sind Verfahren zur Auflösung von Kollisionen möglich. Verfahren, bei denen die übertragenen Zeichen aus Überlagerungsergebnissen berechnet werden, werden als **überlagerndes Empfangen** bezeichnet.

Bei der *Kollisionsauflösung mit Mittelwertbildung und überlagerndem Empfangen* [Pfitzmann 1990] wird für die Menge der *zulässigen* Zeichen $\{0, \ldots, N_{\max}\} \subset \mathbb{Z}$ als Alphabet der Ring $G := \mathbb{Z}/m\mathbb{Z}$ mit $m > n \cdot N_{\max}$ gewählt. Eine Nachricht besteht aus zwei Zeichen. Bei einem Teilnehmer der nicht senden will, sind beide Zeichen 0; bei einem sendewilligen Teilnehmer ist das erste 1, das zweite stellt die eigentliche Nachricht dar. Ist in der empfangenen Nachricht (s, S) das erste Zeichen $s = 1$, wurde die Nachricht S kollisionsfrei übertragen. Andernfalls wird die Menge der Teilnehmer mit Hilfe des Mittelwerts $N := \lfloor S/s \rfloor$ der Nachrichten in zwei disjunkte Teilmengen $P_1 := \{\mathsf{T}_i\colon\ N_i \leq N\}$ und $P_2 := \{\mathsf{T}_i\colon\ N_i > N\}$ aufgeteilt. Die Mittelwertbildung ist möglich, da S auch die Summe der Zeichen in $\mathbb{Z}$ ist. Die Teilnehmer aus P_1 wiederholen ihre Nachrichten $(1, N_i)$ im folgenden Slot. Damit empfangen alle Teilnehmer die Summe (s_1, S_1) der Nachrichten der Teilnehmer aus P_1 und können die Summe der Nachrichten aus P_2 als $(s_2, S_2) := (s - s_1, S - S_1)$ berechnen. Falls $s_2 = 0$, haben alle Teilnehmer dieselbe Nachricht $N_i = N$ gesendet, andernfalls sind beide Teilmengen nicht leer. Der Auflösungsalgorithmus wird dann rekursiv auf beide Teilmengen angewandt. Eine Kollision von s Nachrichten kann so in maximal s Slots (also $s(\lceil \log_2(n) \rceil + \lceil \log_2(N_{\max}) \rceil$ Bits) aufgelöst werden, da in jedem Schritt mindestens eine Nachricht kleiner und eine größer als der Mittelwert ist.

5.4.5 Robustheit

Ein Protokoll ist robust, wenn ein Angreifer die ehrlichen Teilnehmer nicht dauerhaft am Kommunizieren hindern kann [Pfitzmann 1991]. Soll Robustheit garantiert werden, ist Unbeobachtbarkeit nur unter der Voraussetzung möglich, daß jede Nachricht, die ein

Teilnehmer einem anderen sendet, nach beschränkter Zeit tatsächlich ankommt *(Zusammenhangsannahme)* [Pfitzmann 1991]. Diese Anforderung ist schwächer als die der konsistenten Verteilung; sie ist im Internet jedoch nicht erfüllt.

Interne Angriffe lassen sich durch den Einsatz von *Fallenprotokollen* [Chaum 1981, Pfitzmann 1991] aufdecken, so daß der Verursacher der Störung ausgeschlossen werden kann. Dadurch erhöht sich allerdings die Komplexität des Protokolls und der Aufwand für die Teilnehmer. Daher wurde auch vorgeschlagen, absichtliche Störungen nicht anders als Netzausfälle zu behandeln [McCoy 1997].

5.4.6 Effizienz

Der Aufwand für die Schlüsselerzeugung mit kryptographischen Pseudozufallsgeneratoren und das DC^+-Verfahren kann bei Bedarf durch eine geeignete Wahl des Schlüsselgraphen reduziert werden. Die Nutzungsmöglichkeiten von DC-Netzen sind vor allem durch den Aufwand der nötigen Datenübertragung eingeschränkt.

5.4.6.1 Einsetzbarkeit im Internet

Wird das Verfahren auf TCP aufgesetzt, gewährleistet das zugrundeliegende Netz, daß die Daten in der Reihenfolge fehlerfrei eintreffen, in der sie gesendet wurden; es ist aber nicht sichergestellt, daß sie zu einem bestimmten Zeitpunkt tatsächlich eintreffen.

Die Topologie eines DC-Netzes hängt nicht von der des zugrundeliegenden Kommunikationsnetzes ab; Teilnehmer, die über einen gemeinsamen Schlüssel verfügen, müssen nicht mehr direkt miteinander kommunizieren, nachdem sie einen Schlüssel vereinbart haben. Die Teilnehmer können ihre lokale Ausgabe direkt an einen zentralen Knoten senden, der die globale Summe berechnet und an die Teilnehmer verteilt.

Abhängig von der Netzstruktur kann eine Baumstruktur für die Kommunikation der DC-Netz-Teilnehmer sinnvoller sein. Dabei bildet in jedem lokalen Netz ein Knoten die Summe der lokalen Ausgaben der Teilnehmer und gibt sie an einen übergeordneten Knoten weiter; entsprechend erfolgt die Verteilung der globalen Summe. Wenn sich in einem lokalen Netz jeweils viele Teilnehmer befinden, müssen vergleichsweise wenig Daten über die schmalbandigen Verbindungen zwischen den lokalen Netzen übertragen werden.

Ein DC-Netz ist so langsam wie die langsamste Verbindung eines Teilnehmers mit dem Knoten, der die globale Summe berechnet. Ein DC-Netz mit vielen Teilnehmern, das auf einer unzuverlässigen Netzinfrastruktur beruht, ist daher für interaktive Anwendungen wenig geeignet.

Die Nutzbarkeit eines DC-Netzes ist, besonders für Teilnehmer mit schmalbandigem Netzanschluß, auch durch die Menge der zu übertragenden Daten begrenzt. Jeder Teilnehmer muß mindestens so viele Daten übertragen, wie alle zusammen senden wollen. Dieses Problem läßt sich aber lösen, indem das DC-Netz in Slots eingeteilt wird und Teilnehmer mit geringer Übertragungskapazität nur in bestimmten Slots senden.

`To:` S_1	V_1	1	0	0	0	1	1	0	1	1	1	0	1	1	0	0
`To:` S_2	V_2	0	1	0	1	1	0	0	1	0	1	0	0	1	1	1
`To:` S_3	V_3	1	1	0	1	1	1	0	0	1	0	0	1	0	1	1
$V_1 \oplus V_2 \oplus V_3$		0	0	0	0	1	0	0	0	0	0	0	0	0	0	0

Abbildung 5.2: Auswahl durch Bitvektoren

Das DC-Netz dürfte demzufolge besonders für Anwendungen mit sehr hohen Sicherheitsanforderungen, beispielsweise elektronische Wahlen, geeignet sein; es kann aber auch in Netzen mit hoher Bandbreite eingesetzt werden.

5.5 Blinded read

Blinded read [Cooper 1995] ist ein Verfahren für unbeobachtbare Datenbankzugriffe, das zum Abruf von Nachrichten genutzt werden kann.

Die Daten werden in Servern $S_1, S_2, \ldots$ mit identischem Speicherinhalt gespeichert. Der Nutzer sendet an n verschiedene Server individuelle verschlüsselte Anfragen. Aus der Gesamtheit der verschlüsselten Antworten kann er die abgerufene Nachricht berechnen. Sofern mindestens einer der verwendeten Server vertrauenswürdig ist, erhält ein Angreifer keine Informationen darüber, welche Nachricht der Nutzer abgerufen hat.

Durch einen Bitvektor kann eine beliebige Teilmenge der Nachrichten ausgewählt werden. Für Server S_1 bis S_{n-1} wählt der Nutzer jede der Nachrichten mit Wahrscheinlichkeit $p = 1/2$ aus; jeder Server sendet die Exklusiv-Oder-Verknüpfung aller ausgewählten Nachrichten. Für S_n bildet er die Exklusiv-Oder-Verknüpfung der $n - 1$ Auswahlvektoren mit dem Index der gewünschten Nachricht.

Die Exklusiv-Oder-Verknüpfung aller empfangenen Nachrichten ergibt die gewünschte Nachricht (siehe Abb. 5.2). Ohne Kooperation aller Server ist es unmöglich, herauszufinden, welche Mitteilung empfangen wurde.

Dieses Verfahren kann zum anonymen Abruf von Nachrichten eingesetzt werden, indem alle Nachrichten mit einer impliziten Adresse versehen an einen ausgewählten Server gesendet werden. Dieser speichert die Nachrichten, leitet sie regelmäßig in Listen zusammengefaßt an die anderen Server weiter und verteilt eine Liste der impliziten Adressen an alle Teilnehmer.

Der Nutzer sendet Abrufnachrichten an die Server, denen er vertraut; aus den Antworten bildet er die abgerufene Mitteilung. Die Zahl der Abrufnachrichten muß er unabhängig von der Anzahl der an ihn adressierten Mitteilungen wählen.

Wenn nicht alle Server dieselben Daten enthalten, sind die resultierenden Nachrichten nicht lesbar, die Anonymität der Nutzer ist dadurch jedoch nicht gefährdet.

Denial-of-service-Angriffe gegen einzelne Nutzer sind möglich, indem die Liste der impliziten Adressen inkonsistent verteilt wird, und indem die Kommunikation zwischen dem Nutzer und einem Server unterbrochen wird. Auch Server können den Abruf stören, indem sie dem Nutzer ungültige Daten senden. Wenn die Server die Nachrichten vor dem Verschlüsseln signieren, kann der Nutzer bei Bedarf feststellen und gegenüber Dritten nachweisen, welcher Server die Übertragung gestört hat.

Blinded read ist in vielen Anwendungsszenarien effizienter als die Verteilung von Nachrichten, da nur die Adreßdaten an alle Teilnehmer verteilt werden müssen. Die Nutzdaten werden nur an die Server verteilt, wobei die Konsistenz der Verteilung nicht erforderlich ist, um die Anonymität zu gewährleisten.

Kapitel 6

Das Mix-Netz

Ein *Mix* ist ein Netzknoten, der Nachrichten weiterleitet, wobei er den Zusammenhang zwischen seinen Ein- und Ausgaben durch Umkodieren verbirgt [Chaum 1981, Franz 1997]. Wenn eine Mitteilung eine *Sequenz* von unabhängig betriebenen Mixen durchläuft, reicht es aus, daß einer der Mixe vertrauenswürdig ist, um Anonymität und Unbeobachtbarkeit der Kommunikationsbeziehungen zu gewährleisten. Der Angreifer darf mit allen anderen Mixen kooperieren und sämtliche Kommunikationsverbindungen abhören. Realisiert werden Mixe durch den Einsatz asymmetrischer Verschlüsselung.

Hierdurch ergibt sich ein effizientes, gegen mächtige Angreifer sicheres Anonymisierungsverfahren.

6.1 Sender-Anonymität

Zu jedem Mix gehört eine Adresse M_j, ein öffentlicher Schlüssel e_j und ein privater Schlüssel d_j. Will Sender A dem Empfänger B eine Mitteilung m zukommen lassen, wählt er einen beliebigen Pfad $\mathsf{M}_1, \mathsf{M}_2, \mathsf{M}_3, \ldots \mathsf{M}_\lambda$ durch das Mix-Netz, wobei ein Mix auch mehrfach vorkommen kann, und bildet die Nachricht N_1:
$N_\lambda = E_{e_\lambda}(\mathsf{B}, m)$
$N_i = E_{e_i}(\mathsf{M}_{i+1}, N_{i+1}) \quad$ für $i = \lambda - 1, \ldots, 1$
A sendet also $N_1 = E_{e_1}\left(\mathsf{M}_2, E_{e_2}\left(\mathsf{M}_3, E_{e_3}\left(\ldots\left(E_{e_\lambda}\left(\mathsf{B}, m\right)\right)\ldots\right)\right)\right)$ an M_1.

E ist dabei ein gegen aktive Angriffe sicherer probabilistischer Verschlüsselungsalgorithmus. Die Sicherheit gegen *chosen-ciphertext*-Angriffe (siehe Abschnitt 5.2.2) ist erforderlich, da Mixe automatisch beliebige Nachrichten entschlüsseln und das Ergebnis weiterleiten.

Mix M_j sammelt empfangene Nachrichten, bis mehrere der gleichen Länge vorliegen. Für jede Nachricht berechnet er dann $D_{d_j}(N_j) = (\mathsf{M}_{j+1}, N_{j+1})$ und sendet

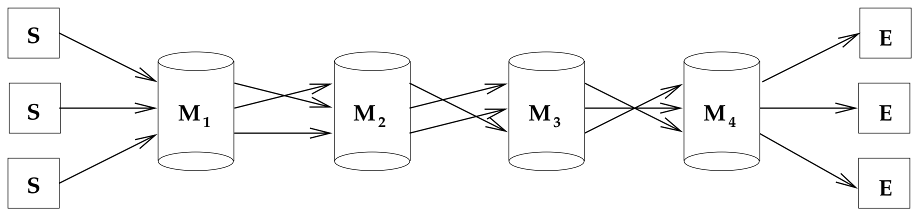


Abbildung 6.1: Schutz der Kommunikationsbeziehung durch eine Mix-Kaskade

die resultierenden Nachrichten in veränderter Reihenfolge an den jeweils angegebenen Mix weiter. Der letzte Mix der Sequenz erhält $D_{d_j}(N_j) = (\mathsf{B}, m)$ und sendet die Nachricht m an B.

Forward secrecy läßt sich durch zusätzliche Verbindungsverschlüsselung zwischen den Mixen sowie zwischen dem Sender und dem ersten Mix erreichen.

Der Teil der Nachricht, der die Adresse und in der Regel weitere für den Mix bestimmte Informationen – beispielsweise einen der Integritätsprüfung dienenden Hash-Wert der Nachricht – enthält, wird als Nachrichtenkopf bezeichnet.

6.1.1 Zuordenbarkeit der Nachrichten

Für einen nicht mit M_j kooperierenden passiven Angreifer E sind die Nachrichten durch ihre *Länge,* durch die verschlüsselten – ohne Kenntnis der geheimen Schlüssel wie zufällig wirkenden – *Daten* und ihren *Ein-* und *Ausgangszeitpunkt* im Mix charakterisiert.

6.1.1.1 Umkodierung

Könnte der Angreifer eine Ausgabe mit größerer Wahrscheinlichkeit als durch zufälliges Auswählen einer Eingabe zuordnen, wären die Annahmen über das zugrundegelegte Kryptosystem verletzt [Rackoff 1993]. Wenn das Kryptosystem sicher ist, kann der Angreifer einem Geheimtext, also der Eingabe eines Mixes, keine Informationen über den zugehörigen Klartext – die Ausgabe des Mixes – entnehmen.

Umgekehrt ist es nicht möglich, den zu einem Klartext gehörenden Geheimtext zu identifizieren, weil die Verschlüsselung probabilistisch ist. Wenn allerdings ein Angreifer eine Nachricht aufzeichnet und wiederholt an den Mix sendet ist die Voraussetzung, daß der Geheimtext zufällig ausgewählt wird, nicht erfüllt. Das wiederholte Senden identischer Eingaben *(Replay-Angriff)* an einen Mix führt zu identischen Ausgaben; die Zuordnung ist damit trivial. Um dies zu verhindern, muß der Mix Wiederholungen ignorieren.

6.1.1.2 Wiederholungen

Zum Erkennen von Wiederholungen kann der Mix ein eindeutiges oder jedenfalls nur mit vernachlässigbarer Wahrscheinlichkeit mehrfach auftretendes Merkmal jeder bearbeiteten Nachricht in einer Datenbank speichern. Das Prüfen auf Wiederholung entspricht dann einem Datenbankzugriff. Da alle während der Gültigkeitsdauer eines Schlüsselpaares weitergeleiteten Nachrichten in der Datenbank vermerkt werden müssen, ist der Speicherplatzbedarf dieses Verfahrens groß. Wenn die Nachricht nur innerhalb eines bestimmten Zeitraums eintreffen kann, reicht es aus, einen im mit E_{e_j} verschlüsselten Teil der Nachricht enthaltenen Zeitstempel zu prüfen und nur neuere Nachrichten nach Abgleich mit der Datenbank zu akzeptieren. Einträge in der Datenbank können dann nach Ablauf der zulässigen Zeitspanne gelöscht werden [Gülcü 1996].

Enthält der Nachrichtenkopf jeweils eine vom Sender für jeden Mix aus einem hinreichend großen Merkmalsraum zufällig gewählte `Message-ID`, treten Kollisionen nur mit geringer Wahrscheinlichkeit auf.

6.1.1.3 Nachrichtenlänge

Bei der Entschlüsselung entfernt der Mix den Sitzungsschlüssel sowie die Adreßinformation aus dem Datenpaket. Die Nachricht wird dadurch kürzer. Sofern nicht für alle Nachrichten ein vorgegebener Pfad *(Kaskade)* verwendet wird, muß die Umkodierung *längentreu* erfolgen, um Angreifern keine Information über den Weg der Nachricht zu geben [Pfitzmann 1990]. Dazu ergänzt der Mix die Nachricht bis zur ursprünglichen Länge mit zufälligen Bits *(padding)*. Da weder ein passiver Angreifer noch die folgenden Mixe – bei unverschlüsseltem m mit Ausnahme des letzten oder der mit ihm kooperierenden Mixe – die zur Entschlüsselung nötigen Schlüssel kennen, können sie das Padding nicht von verschlüsselten Nutzdaten unterscheiden. Um zu verhindern, daß die Padding-Länge nach dem Durchlaufen der Mix-Sequenz Informationen über die Länge des Pfades enthält, kann eine maximale Pfadlänge für das Gesamtsystem festgelegt werden. Die reservierten und nicht genutzten Einträge füllt dabei schon der Sender mit zufälligen Bits auf.

Durch diese Umkodierung werden die Nachrichten somit nach ihrer Länge in Klassen eingeteilt, innerhalb derer sie anonym und unbeobachtbar sind. Um eine von der Nachrichtenlänge unabhängige Anonymitätsmenge zu erhalten, kann für alle Nachrichten eine einheitliche Länge festgelegt werden. Längere Mitteilungen muß der Absender dann in mehrere Nachrichten aufteilen; alle Nachrichten werden bis zur festgesetzten Länge mit zufälligen Bits aufgefüllt.

6.1.1.4 Umsortierung

Um die Unsicherheit über den Zusammenhang zwischen Ein- und Ausgabe zu erhöhen, müssen genügend viele Nachrichten gesammelt werden. Die Reihenfolge des Aussendens darf keine Informationen über die Reihenfolge des Empfangens der Nachrichten preisgeben. Für das Sammeln und Umsortieren der Nachrichten sind verschiedene, zeit- oder ereignisorientierte Strategien möglich.

Im *Batch-Betrieb* sammelt ein Mix mindestens N Nachrichten an, die dann in beispielsweise lexikographischer Reihenfolge in einem Schub ausgegeben werden [Chaum 1981]. Im *Intervall-Batch-Betrieb* [Gülcü 1996] wird jeweils nach Ablauf eines festgelegten Zeitraums T ein Nachrichtenschub ausgegeben. Falls während des Intervalls nur $n < N$ Nachrichten eingetroffen sind, erzeugt der Mix $N - n$ bedeutungslose Nachrichten *(dummy messages).* Damit ist T die maximale und $T/2$ die durchschnittliche Verzögerungszeit für eine Nachricht.

Eine andere Möglichkeit stellt der *Pool-Betrieb* dar. In dieser Betriebsart wird, sobald die N-te Nachricht eintrifft, zufällig eine Nachricht ausgewählt und weiterverarbeitet [Franz 1997]. In diesem Fall ist die Verzögerung hinsichtlich eines Zählers, der jeweils beim Eintreffen einer neuen Nachricht erhöht wird, geometrisch verteilt: $\mathrm{P}(\{T = k\}) = (1 - \frac{1}{N})^{k-1}\frac{1}{N}$. Der Erwartungswert ist $E(T) = N$, d. h. eine Nachricht bleibt im Durchschnitt bis zum Eintreffen N weiterer Nachrichten gespeichert.

Möglich ist auch der *Intervall-Pool-Betrieb.* In dieser Betriebsart wird jeweils nach Ablauf eines festgelegten Zeitraums geprüft, wieviele Nachrichten im Pool gespeichert sind. Enthält der Pool $n > N$ Nachrichten, werden nacheinander $n - N$ Nachrichten zufällig ausgewählt und bearbeitet. Andernfalls werden keine Nachrichten bearbeitet. In einer Variante mit *variabler Pool-Größe* werden in jedem Intervall nur $c(n - N)$ Nachrichten bearbeitet, $0 < c < 1$. Der Pool hat somit eine Mindestgröße; wenn mit gleichbleibender Häufigkeit Nachrichten eintreffen, ergibt sich für eine (möglicherweise größere) Poolgröße ein Gleichgewicht. Bei einem plötzlichen Ansteigen des Netzverkehrs wird der Pool größer.

6.1.2 Grad der Anonymität

Ein Angreifer kann die Eingabe und die Ausgabe des Mixes beobachten. $\mathcal{G}$ bezeichne die Wahrscheinlichkeit, daß Angreifer E eine Nachricht anhand dieser Beobachtung korrekt dem Sender A zuordnet. Je größer die vom Mix erzielte *Konfusion,* desto kleiner ist $\mathcal{G}$.

S_I sei die Anzahl der von I im betrachteten Zeitraum an den Mix gesendeten Nachrichten ($I = \mathsf{A}$ oder $I = \mathsf{E}$). Für einen im Batch-Betrieb arbeitenden Mix gilt dann:

$$\mathcal{G} = \frac{S_{\mathsf{A}}}{N - S_{\mathsf{E}}} \tag{6.1}$$

Im Batch-Intervall-Betrieb ist bei n Dummy-Nachrichten:

$$\mathcal{G} = \frac{S_{\mathsf{A}}}{N - S_{\mathsf{E}} - n} \tag{6.2}$$

Diese Betriebsart ist daher bei wenig Verkehr im Netz unsicher.

Im Pool-Betrieb wird jede gespeicherte Nachricht beim Eintreffen jeder neuen Nachricht mit Wahrscheinlichkeit $1/N$ weiterbearbeitet. Die Wahrscheinlichkeit, daß

Nachrichten sehr lange im Pool bleiben, ist gering. Ein Angreifer kann daher ein – hinreichend großes – Intervall betrachten und ältere Nachrichten vernachlässigen.

Die Sicherheit des Mixes beruht somit in allen Betriebsarten darauf, daß N ausreichend groß ist. Bei gleich vielen eintreffenden Nachrichten führt ein größeres N jedoch zu höheren Verzögerungszeiten. Je mehr Nachrichten durch den Mix anonymisiert werden, desto größer kann N werden, ohne zu einer inakzeptablen Verzögerung zu führen.

6.1.3 Effizienz

Der Sender muß λ Verschlüsselungsoperationen durchführen, jeder Mix für jede durch ihn gesendete Nachricht eine Entschlüsselung. Das zugrundeliegende Kommunikationsnetz muß je Mitteilung λ Nachrichten fester Größe übertragen.

Entscheidend für die Effizienz des Verfahrens sind die auftretenden Verzögerungszeiten, die von der Pfadlänge und der Betriebsart des Mixes abhängen. Mit Ausnahme des Intervall-Batch-Betriebs wird eine Nachricht verzögert ausgegeben, falls die Ausgabe nicht möglich ist, ohne die Anonymität des Senders zu gefährden. Wenn der in der Nachricht enthaltene Zeitstempel dadurch ungültig wird, geht die Nachricht verloren.

6.1.4 Mix-Sequenzen

Wird mehr als ein Mix eingesetzt, erhöht sich die Zahl der geheimen Schlüssel, die kompromittiert werden müssen, um den Sender zu identifizieren.

Ist für alle Mitteilungen ein fester Pfad vorgegeben, können die Nachrichten kürzer sein, da keine Adreßangaben für die folgenden Mixe und kein Padding für eventuelle nicht ausgenutzte Pfadlängen erforderlich sind. Da jeder Mix innerhalb der Kaskade nur Nachrichten von seinem Vorgänger erhält und an seinen Nachfolger sendet, ist das Mix-Netz einfacher zu verwalten und zuverlässiger, als wenn jeder Mix mit jedem anderen Nachrichten austauschen müßte [Gülcü 1996]. Auch ergeben sich kürzere Übertragungszeiten, da jeder Mix seinem Nachfolger einen bereits vollständigen Batch sendet.

Eine Mix-Kaskade mit Batchgröße N wird von N Nachrichten parallel durchlaufen. Somit ist wie bei einem einzelnen Mix $\mathcal{G} = \sum_{i=t-N}^{t} \mathrm{P}(S_{i,\mathtt{A}})/N$. Durch die Verwendung einer Kaskade erhöht sich also – sofern sie mehrere vertrauenswürdige Mixe enthält, die Sicherheit – nicht aber die Konfusion.

In einem System mit vielen Mixen ist es ineffizient, jede Nachricht durch alle Mixe zu senden. In dem Fall sollte der Nutzer die Möglichkeit haben, Mixe auf der Basis der Topologie des zugrundeliegenden Kommunikationsnetzes und seines Vertrauens zu wählen. Die Eingaben der Mixe sind dann von einander verschieden. Die resultierende Konfusion kann daher bei gegebener Batchgröße größer sein als bei einem einzelnen Mix. In [Rackoff 1993] wird gezeigt, daß eine vor passiven Angreifern verborgene Permutation von n Nachrichten, also $\mathcal{G} = 1/n$, bei n Mixen der Batchgröße $N = 2$ bei in $\log(n)$ polynomiellen Pfadlängen erreicht werden kann.

Im Intervall-Batch-Betrieb ergeben sich wie bei Mix-Kaskaden kurze Übertragungszeiten, da die Takte der aufeinander folgenden Mixe aufeinander abgestimmt werden können. Im ereignisgesteuerten Batch-Betrieb und im Pool-Betrieb werden Nachrichten in jedem Mix verzögert. Der Erwartungswert der Verzögerungszeit steigt dabei proportional zur Pfadlänge.

6.1.5 Verkehrsanalyse

Auch wenn ein Mix oder ein Mix-Netz vertrauenswürdig und sicher ist, also vollkommene Konfusion unter N Nachrichten erzielt, kann ein Angreifer Informationen über die Nutzer gewinnen. Die Zahl der von A an Mixe gesendeten Nachrichten ist die obere Grenze für die Zahl der Mitteilungen von A; eine Differenz zur Zahl der tatsächlichen Mitteilungen entsteht nur, indem A Dummy-Nachrichten generiert [Rackoff 1993].

Im Fall einer einmaligen Nachricht ergibt sich bei einem sicheren Mix: $\mathcal{G} = 1/N$, d. h. A ist *außer Verdacht* (Abschnitt 3.4.1) in der Menge aller Sender des Intervalls.

Benutzt A ein Pseudonym, sind die anonymen Nachrichten verkettbar. Die Anonymitätsmenge wird dann durch wiederholte Durchschnittbildung kleiner. A ist anonym bezüglich der Menge $\mathcal{A}'$ aller Sender, die in jedem Intervall, in dem A n_i pseudonyme Mitteilungen gesendet hat, mindestens n_i Nachrichten gesendet haben. Es gilt: $\mathcal{G} = 1/\left|\mathcal{A}'\right|$. $\mathcal{A}'$ ist unter Umständen erheblich kleiner als $\mathcal{A}$.

Die Unbeobachtbarkeit einer Kommunikationsbeziehung kann in ähnlicher Weise eingeschränkt werden [Dai 1995]. Der Angreifer bildet für jedes Intervall i das Minimum $m_{\mathsf{AB},i}$ der Zahl der von A gesendeten und der von B empfangenen Nachrichten. $m_{\mathsf{AB},i}$ ist die obere Grenze für die Zahl der Nachrichten, die A in diesem Intervall an B geschickt haben kann. Wenn $\sum_{i \in T} m_{\mathsf{AB},i}$ in einem Beobachtungszeitraum T größer ist als $\sum_{i \in T} m_{\mathsf{A}I,i}$ für alle $I \in \mathcal{A} \setminus \{\mathsf{B}\}$, kann der Angreifer erkennen, daß die Kommunikation stattfindet. Ob dies möglich ist, hängt vom Verhalten von A und B und dem der anderen Nutzer ab.

Gegen diese Verkehrsanalyse können die Nutzer sich schützen, indem sie unabhängig von tatsächlichen Sendewünschen in festen Takten Nachrichten senden. Die Zahl dieser Nachrichten begrenzt die Anzahl der Mitteilungen, die ein Nutzer zu einem gegebenen Zeitpunkt senden kann; will er weniger senden, erzeugt er Dummy-Nachrichten. Auch wenn der Nutzer selbst einen Mix betreibt, der auch von anderen genutzt wird, ist keine Verkehrsanalyse möglich.

6.1.6 Aktive Angriffe

Ein aktiver Angreifer kann Nachrichten unterdrücken, fälschen und verändern. Angriffe durch das Unterdrücken von Nachrichten sind im Mix-Netz möglich; gegen Angriffe durch verfälschte Nachrichten kann es gesichert werden.

6.1.6.1 Verändern von Nachrichten

Wenn, wie bei Verschlüsselung im ECB-Modus, identische Geheimtextblöcke zu identischen Klartextblöcken führen, ist ein aktiver Angriff durch Verfälschen von an Mixe gerichteten Nachrichten möglich: Der Angreifer dupliziert einen Block einer Nachricht an einer anderen Stelle und prüft, welche der Ausgabenachrichten das entsprechende Muster aufweist. Falls der Angreifer eine Nachricht verkürzt, indem er beispielsweise einen Teil des Paddings abschneidet, darf der Mix nicht eine entsprechend verkürzte umkodierte Nachricht ausgeben. Sonst könnte der Angreifer den Weg der Nachricht anhand ihrer Länge verfolgen. Auch muß es unmöglich sein, Teile der Nachricht so zu ändern, daß das zur Prüfung auf Wiederholung (Abschnitt 6.1.1.2) verwendete Merkmal sich ändert, aber die Steuerung gleichbleibt.

Verhindert werden muß auch, daß ein Angreifer in einer Nachricht Informationen kodiert, die er nach dem Durchlaufen von Mixen der Ausgabenachricht wieder entnehmen kann, um Ein- und Ausgabe einander zuzuordnen. Statt des zufälligen Paddings könnte ein Mix von ihm gewählte Daten in eine Nachricht einfügen oder einen Teil der Nachricht durch von ihm gewählte Daten ersetzen. Informationen lassen sich auf diese Weise nicht in der Nachricht transportieren, da der erste ehrliche Mix der Sequenz die Nachricht mit einem dem Angreifer nicht bekannten Sitzungsschlüssel umkodiert; die Daten sind für den Angreifer nach der Umkodierung also nicht mehr lesbar. Das Verfälschen des Geheimtextes führt aber dazu, daß der zugehörige Klartext von der veränderten Position an nicht mehr lesbar ist; die resultierenden Daten sind pseudozufällig. Schon die Information, daß der Text an einer gegebenen Position verändert wurde, kann einem Angreifer die Zuordnung der Nachricht ermöglichen. Erkennen kann der Angreifer die Veränderung, wenn er den an den Empfänger gesendeten Klartext beobachtet, sowie in den Nachrichtenköpfen, die die mit ihm kooperierenden Mixe empfangen. Somit können ehrliche Mixe überbrückt werden.

Um diesen Angriff zu verhindern, müssen die Mixe anhand eines Hash-Wertes die Integrität der von ihnen bearbeiteten Nachrichten prüfen. Im Nachrichtenkopf muß dazu ein Hash-Wert der verschlüsselten Nachricht sowie des für den jeweiligen Mix bestimmten Teils des Nachrichtenkopfes gespeichert sein. Die verschlüsselten weiteren Teile des Nachrichtenkopfes können (mit Ausnahme des direkt folgenden) nicht geprüft werden, da es sich dabei auch um zufälliges Padding handeln kann. Wenn ein vom Mix berechneter Hash-Wert nicht dem vom Sender angegebenen entspricht, wurde die Nachricht verfälscht und muß verworfen werden.

6.1.6.2 Fälschen von Nachrichten

Vor dem Weiterleiten einer Nachricht prüft der Mix, daß kein Replay-Angriff vorliegt (siehe Abschnitt 6.1.1.2).

Möglicherweise kann ein Angreifer jedoch zu einer an einen Mix gerichteten Nachricht weitere davon abgeleitete Geheimtexte erzeugen und an den Mix senden, so daß der Mix den Zusammenhang nicht feststellen kann. Wenn der Mix diese Eingaben in Ausgaben transformiert, die für den Angreifer erkennbar mit der echten Ausgabenachricht zusammenhängen, kann der Angreifer die zu er Nachricht gehörende

Ausgabe identifizieren und so den Mix überbrücken. Dies ist bei einer direkten RSA-Implementierung von Mixen der Fall [Pfitzmann 1990b]. Dieser Angriff ist nicht möglich, wenn der verwendete Algorithmus *plaintext aware* ist.

6.1.6.3 Isolieren von Nachrichten

Ein Angreifer kann die von einem Mix erzielte Konfusion reduzieren, indem er eine große Anzahl von Nachrichten an den Mix sendet *(flooding).* Da er seine eigenen Nachrichten nach der Umkodierung wiedererkennt, besteht über diese Nachrichten keine Unsicherheit. Kennt er $N-1$ der in einem Schub bearbeiteten N Nachrichten, ist die Zuordnung der N-ten Nachricht trivial. Daher muß verhindert werden, daß ein großer Teil der gleichzeitig bearbeiteten Nachrichten von demselben Absender stammt.

Wie groß der Aufwand für diesen Angriff ist, hängt von der Betriebsart der Mixe ab. Um eine bestimmte Nachricht zu verfolgen, kann der Angreifer sie abfangen und zusammen mit von ihm erzeugten Nachrichten an den Mix senden. Bei einer Mix-Kaskade im Batch-Betrieb muß er dafür $N - 1$ Nachrichten erzeugen, die dann zusammen mit der fraglichen Nachricht die Kaskade durchqueren. Bei einem frei wählbaren Pfad müssen in jedem Mix $N - 1$ Nachrichten vorliegen, wenn die Nachricht dort eintrifft. Der Angreifer muß die Nachricht daher anhalten, sobald sie den Mix verläßt, oder eine insgesamt sehr große Zahl von Nachrichten erzeugen. Besonders viele Nachrichten muß der Angreifer im Intervall-Pool-Betrieb mit variabler Größe senden, bis alle in einem Mix gespeicherten Nachrichten von ihm stammen. Je mehr Nachrichten der Angreifer erzeugen muß, desto größer ist die Wahrscheinlichkeit, daß der Angriff entdeckt wird.

Eine weitere mögliche Maßnahme gegen das Isolieren von Nachrichten besteht darin, mit digitalen Signaturen sicherzustellen, daß die in einem Schub bearbeiteten Nachrichten von verschiedenen Absendern stammen [Franz 1997]. Treffen zu viele Nachrichten von einem Absender ein, oder sind Nachrichten nicht mit einem von einem vertrauenswürdigen Dritten zertifizierten Signaturschlüssel signiert, lehnt der erste Mix diese Nachrichten ab. Die anderen Mixe können an dieser Stelle ebenfalls prüfen, um sicherzustellen, daß der erste Mix korrekt vorgeht. Mixe im Batch-Betrieb können mit einem Zero-Knowledge-Beweis zeigen, daß sie die Nachrichten protokollkonform umkodiert haben [Rackoff 1993]. Eine Möglichkeit für einen solchen Beweis wurde – allerdings beruhend auf einer unsicheren Mix-Netz-Variante [Michels 1996] – in [Sako 1995] vorgeschlagen.

Allerdings läßt sich nicht verhindern, daß mehrere Absender kooperieren. Insbesondere in einem weltweiten offenen Netz bietet dieses Verfahren somit kaum Schutz.

Ein Mix kann die Unsicherheit über die zu einer Eingabe gehörende Ausgabenachricht erhöhen, indem er Dummy-Nachrichten erzeugt. Gegen den Empfänger der Nachricht bieten vom letzten vertrauenswürdigen Mix der Sequenz erzeugte Dummies keinen Schutz, da sie keine Unsicherheit über die Eingabe bewirken [Franz 1997].

Gibt der Mix die umkodierten Nachrichten seinerseits unbeobachtbar aus, kann der Angreifer seine eigenen Nachrichten nicht mehr erkennen. Flooding-Angriffe werden dadurch wirkungslos. Erreichen läßt sich dies, sofern nicht alle Mixe gleichzeitig angegriffen werden, indem der Mix seine Ausgabe durch eine von ihm gewählte Mix-Sequenz weiterleitet (siehe Abschnitt 6.2.1). Derartig umgeleitete Nachrichten müssen gekennzeichnet werden, um Endlosschleifen zu vermeiden. Auch wenn der Mix seine Ausgabe nicht nur an den nächsten Mix sendet, sondern an eine Gruppe von Mixen verteilt, kann der Angreifer den Weg der Nachricht nicht beobachten [Wayner 1996].

6.1.6.4 Unterdrücken von Nachrichten

Vereinfacht werden Flooding-Angriffe, wenn der Angreifer auch legitime Nachrichten unterdrücken kann. Außerdem ermöglicht das Unterdrücken von Nachrichten Angriffe gegen einzelne Teilnehmer.

Ein aktiver Angreifer, der den ersten Mix einer Kaskade oder den Übertragungsweg dorthin kontrolliert und die Ausgabe des letzten Mixes beobachten kann, kann Nachrichten isoliert in das Mix-Netz einspielen und die resultierende Ausgabe beobachten [Gülcü 1996]. Dieser zentrale Angriffspunkt existiert bei Mix-Netzen mit frei wählbarem Pfad nicht: Der Sender kann eine Mitteilung bei verschiedenen Mixen einliefern. Erzeugt er Nachrichten für verschiedene Mixe so, daß nach der Entschlüsselung durch einen Teil der Mixe für den letzten Teilpfad in beiden Fällen dieselbe Nachricht entsteht, erkennt der erste Mix dieses Teilpfads die Wiederholung und ignoriert die als zweite eintreffende Nachricht. Durch die redundante Übertragung wird ein höherer Aufwand zum Unterdrücken der Nachricht erforderlich.

Wenn der Nutzer vom ersten Mix eine signierte Empfangsbestätigung für die eingelieferten Nachrichten erhält, kann er nachweisen, daß seine Eingabe nicht korrekt bearbeitet wurde [Chaum 1981]; die Mixe beweisen ihr protokollkonformes Vorgehen mit einem Zero-Knowledge-Beweis. Für den Pool-Betrieb ist keine maximale Verzögerungszeit festgelegt; daher kann dem Mix nicht nachgewiesen werden, daß er einen Angriff versucht hat [Franz 1997].

Es besteht jedoch auch die Gefahr, daß ein Nutzer aufgrund eines aktiven Angriffs oder auch eines Fehlers des zugrundeliegenden Kommunikationsnetzes keine Verbindung zu Mixen aufbauen kann. Die Möglichkeit, sich dagegen zu schützen, indem im Fehlerfall das gesamte Protokoll abgebrochen wird, ist bei einer großen Teilnehmerzahl nicht praktikabel.

Wenn der Angreifer Nachrichten eines Teilnehmers unterdrückt und zu einem späteren Zeitpunkt gesammelt an den Mix sendet, kann er aus den dann in entsprechend großer Zahl auftretenden anonymen Nachrichten auf die Zuordnung schließen. Die Wirksamkeit dieses Angriffs können Mixe durch das Prüfen eines Zeitstempels in der Nachricht einschränken.

6.2 Empfänger-Anonymität

Empfänger-Anonymität läßt sich durch den Einsatz anonymer Rückadressen erreichen. Die Mixe kodieren auch in diesem Fall Nachrichten um, prüfen auf Wiederholung

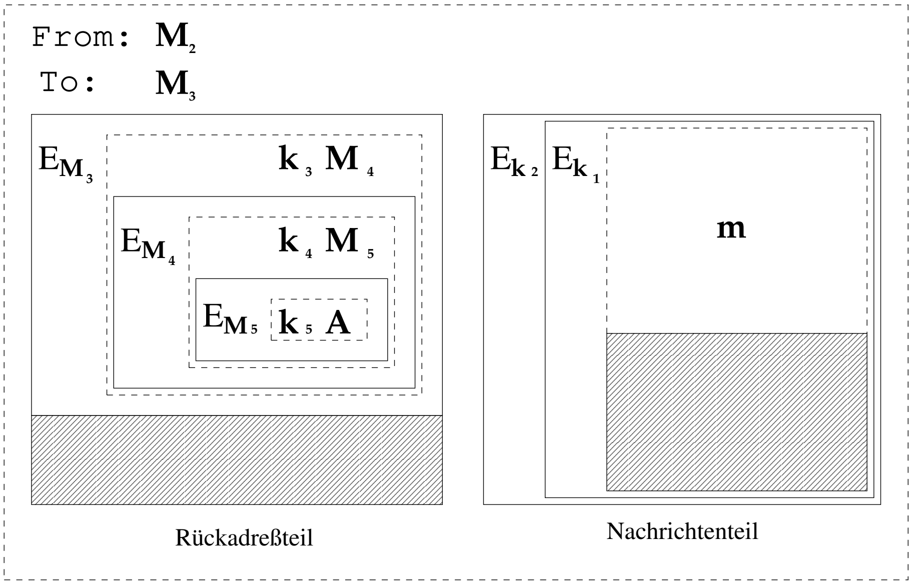


Abbildung 6.2: Verwendung von Mixen zur Empfänger-Anonymität

und geben sie in geänderter Reihenfolge aus; die Umkodierung enthält aber eine Verschlüsselungsoperation. Will der Nutzer A anonym Nachrichten empfangen, wählt er einen Pfad durch das Mix-Netz – ohne Beschränkung der Allgemeinheit sei der Pfad $\mathsf{M}_1, \mathsf{M}_2, \ldots \mathsf{M}_\lambda$ –, generiert symmetrische Schlüssel $k_1, k_2, \ldots k_\lambda$ und bildet die Rückadreß-Information R_1:
$\mathsf{R}_\lambda = E_{e_\lambda}(k_\lambda, \mathsf{A})$
$\mathsf{R}_i = E_{e_i}(k_i, \mathsf{M}_{i+1}, \mathsf{R}i+1) \quad \text{für } i = \lambda - 1, \ldots, 1$
Die Rückadresse $(\mathsf{M}_1, \lceil \mathsf{R}_1 \rceil)$ teilt A seinem Kommunikationspartner B anonym mit. B sendet das Paar $(\lceil \mathsf{R}_1 \rceil, \lceil m \rceil)$ aus der Rückadreß-Information und seiner Nachricht an M_1. $\lceil \cdot \rceil$ bezeichnet dabei Padding auf eine systemweit vorgegebene Größe.

Mix M_j enthält für jede Nachricht (R_j, N_j) durch Entschlüsselung $D_{d_j}(\mathsf{R}_j) = (k_j, \mathsf{M}_{j+1}, \mathsf{R}_{j+1})$ und sendet $(\lceil \mathsf{R}_{j+1} \rceil, E_{k_j}(N_j))$ an M_{j+1}.

Der letzte Mix M_λ erhält $D_{d_\lambda}(\mathsf{R}_\lambda) = (k_\lambda, \mathsf{A})$ und sendet $E_{k_\lambda}(N_\lambda)$ an A. A entschlüsselt diese Nachricht $E_{k_\lambda}(E_{k_{\lambda-1}}(\ldots E_{k_1}(m)\ldots))$ mit den von ihm erzeugten symmetrischen Schlüsseln und erhält so die von B gesendete Mitteilung m.

Da die Mixe die Rückadreß-Informationen auf Wiederholungen prüfen und gegebenenfalls ignorieren müssen, kann jede anonyme Rückadresse nur einmal verwendet werden. Daher ist es nicht ohne weiteres möglich, einem anonymen Empfänger mehrere Nachrichten zu senden. Da zwischen dem Erzeugen der Rückadresse und dem Senden der Nachricht ein größerer Zeitraum liegen kann, werden die Datenbanken der Mixe zur Wiederholungsprüfung groß. Da in einem großen Zeitraum die Wahrscheinlichkeit hoch ist, daß ein Mix den Betrieb einstellt oder seinen Schlüssel wechselt, sinkt die Zuverlässigkeit des Mix-Netzes.

Um diese Probleme zu beheben, wurden *Umleitungen* zwischen Mixen und das Verfahren des *anonymen Abrufs* vorgeschlagen.

6.2.1 Umleitung zwischen Mixen

Wenn ein Mix seine Ausgabe-Nachrichten durch jeweils zufällig gewählte Mix-Sequenzen (Umleitung, *Inter-Mix Detour)* weiterleitet, führen identische Eingaben zu verschiedenen Ausgaben [Gülcü 1996]. Die Wirkung eines Replay-Angriffs wird damit reduziert. Wird dann auf die Prüfung auf Wiederholung verzichtet, können beliebig viele anonyme Nachrichten an eine anonyme Rückadresse gesendet werden.

Wenn nur ein Mix vertrauenswürdig ist, wird durch Umleitungen keine zusätzliche Sicherheit erreicht. Für den sendenden Mix selbst entsteht keine Unsicherheit, wenn er seine Ausgabe über eine Umleitung ausgibt. Auch wenn die von einem vertrauenswürdigen Mix als Umleitung ausgewählten Mixe mit dem Angreifer kooperieren, verursacht die Umleitung dem Angreifer keine zusätzliche Unsicherheit.

Aber auch wenn alle Mixe vertrauenswürdig sind, ist dieses Verfahren nicht sicher gegen Replay-Angriffe, da identische Eingaben nach dem Durchlaufen der Umleitung wieder zu identischen Ausgaben führen. Sendet der Angreifer eine Nachricht mehrfach an eine anonyme Adresse, dann erhält der Empfänger entsprechend viele identische verschlüsselte Nachrichten. Die Anonymität läßt sich somit aufdecken.

6.2.2 Anonymer Abruf

Größere Sicherheit bietet der *anonyme Abruf* [Pfitzmann 1990]. Hierfür wählt A ein Pseudonym P, sendet einen für dieses Pseudonym generierten Schlüssel d_P an einen *Pseudonym-Server* und teilt B seine pseudonyme Adresse mit. Der Server speichert die für P eingehenden Nachrichten. Wenn A ihm eine mit d_P authentisierte anonyme Rückadresse sendet, leitet er die gespeicherten Nachrichten an die angegebene anonyme Adresse weiter (siehe Abb. 6.3).

A kann seine Nachrichten so regelmäßig abrufen. Um die Anfragen an den Server zu senden, setzt A das Verfahren zur Sender-Anonymität ein; die Antworten erfolgen durch das Verfahren zur Empfänger-Anonymität. A ist daher auch gegenüber dem Server anonym. Da für jeden Abruf eine neue Rückadresse verwendet wird, sind Prüfungen auf Wiederholung möglich. Da der Server die Antwort sofort sendet, muß die Rückadresse nur kurzfristig gültig sein.

Geeignet ist dieses Verfahren vor allem für E-Mail. Wollte A für einen interaktiven Dienst, z. B. telefonisch, anonym erreichbar sein, müßte er in hoher Frequenz Abruf-Nachrichten versenden. Für den Verbindungsaufbau könnte Empfänger-Anonymität durch Verteilung somit effizienter sein.

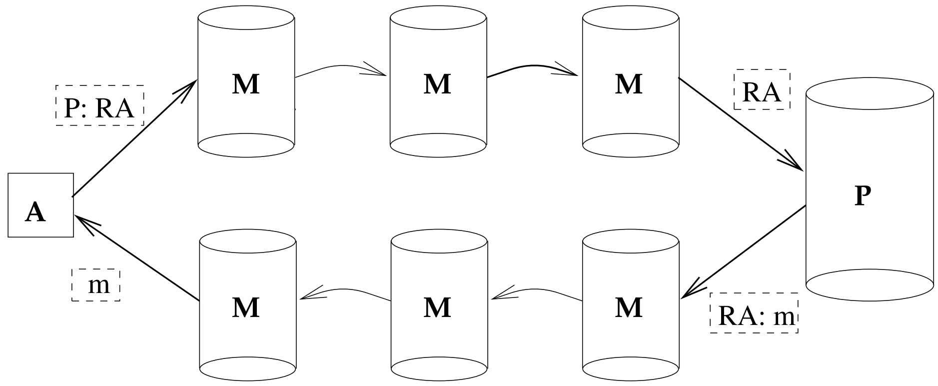


Abbildung 6.3: Anonymer Abruf

6.3 Anwendung für E-Mail

Zur Anwendung für E-Mail existieren die Mix-Netz-Implementationen Mixmaster [Cottrell 1995] und BABEL [Gülcü 1996].

6.3.1 Mixmaster

Mixmaster dient der Anonymisierung von E-Mail. Implementiert ist derzeit nur Sender-Anonymität. Die Nachrichten werden bei einer Schlüssellänge von 1024 Bit mit RSA nach PKCS # 1 [RSA 1993] und 3DES mit 168-Bit-Schlüsseln verschlüsselt. Die Mitteilungen haben eine feste Größe von 10kB; längere Mitteilungen werden in mehrere Teile unterteilt und vom letzten Mix wieder zusammengesetzt. Im Nachrichtenkopf der verschlüsselten Nachrichten ist Speicherplatz für eine Pfadlänge von 20 Mixen vorgesehen; jeder Eintrag ist 512 Bytes lang. Nicht ausgenutzter Platz wird mit zufälligem Padding aufgefüllt. Durch die für E-Mail bei verschlüsselten Daten erforderliche Radix-64-Transportkodierung [Linn 1993] ergibt sich eine Gesamtlänge von 28kB.

Zum Erzeugen der Nachrichten wird ein eigenes ClientProgramm verwendet. Die Mixe können unter Berücksichtigung ihrer aktuellen Zuverlässigkeit [EFGA 1998] zufällig oder vom Benutzer ausgewählt werden. Zur Erhöhung der Verläßlichkeit ist es möglich, für eine Nachricht verschiedene Pfade zu verwenden. Der letzte Mix muß bei allen Pfaden identisch sein, so daß Wiederholungen erkennt und die Nachricht nur einmal ausgeliefert wird.

Zum Schutz gegen Replay-Angriffe prüfen die Mixe die Gültigkeit der empfangenen Nachrichten anhand eines Zeitstempels und vom Sender erzeugten Paket-IDs. Mixmaster verwendet einen *Pool* konfigurierbarer Größe, der jeweils beim Eintreffen einer neuen Nachricht oder nach einem festgelegten Intervall bearbeitet wird. Um Flooding-Angriffe zu erschweren und eine gleichmäßigere Auslastung des Systems zu erreichen, ist auch eine *variable Poolgröße* möglich. Das Isolieren von Nachrichten ist daher nur mit hohem Aufwand möglich.

Nach Abgleich mit einer Sperrliste werden die Nachrichten per E-Mail an den Empfänger ausgeliefert.

6.3.2 BABEL

BABEL ist ein Perl-Programm zur Anonymisierung von E-Mail, das zur Verschlüsselung PGP verwendet. Es erreicht Sender-Anonymität sowie durch Verwendung mehrmals verwendbarer anonymer Rückadressen eingeschränkt sichere Empfänger-Anonymität. Dabei werden zwischen den Mixen *Umleitungen* eingesetzt.

Die maximale Länge für Mitteilungen beträgt 24kB; längere Mitteilungen werden nicht unterstützt. Ein Rückadreß-Block ist 1,5 kB groß, so daß sich als maximale Länge für den Antwortpfad 7 ergibt.

Zum Schutz vor Replay-Angriffen werden aus dem verschlüsselten Sitzungsschlüssel abgeleitete Bezeichner in Kombination mit Zeitstempeln verwendet. BABEL-Remailer werden im Intervall-Batch-Betrieb betrieben.

6.4 Anwendung für interaktive Dienste

Onion Routing [Reed 1996, Syverson 1997] ist ein Verfahren, das das Mix-Prinzip für unbeobachtbare interaktive Verbindungen auf Socket-Ebene verwendet.

Weitere Vorschläge zum interaktiven Einsatz von Mixen sind *Telefon-Mixe* [Pfitzmann 1989] und der *Pipenet*-Entwurf [Goldberg 1997b, McCoy 1997].

Für den Einsatz im ISDN wird nach [Pfitzmann 1989] eine Mix-Kaskade (Telefon-Mixe) in der Ortsvermittlungsstelle verwendet. Die Datenübertragung erfolgt durch Mix-Kanäle; zum Verbindungsaufbau wird Verteilung eingesetzt. Netzanschlüsse, die keine reale Verbindung aufrechterhalten, senden Nachrichten an sich selbst, so daß Zusammenhänge zwischen der Aktivität des Teilnehmers und anonymisierten Gesprächen für Beobachter nicht erkennbar sind. Telefon-Mixe verbergen nur die Kommunikation innerhalb einer Ortsvermittlungsstelle; Dauer und beteiligte Vermittlungsstellen von Ferngesprächen bleiben beobachtbar.

Pipenet gleicht die durch die kurzen Verzögerungzeiten erleichterten zeitabhängigen Angriffe durch eine große Anzahl von Dummy-Nachrichten aus. Zwischen den Mixen bestehen langlebige verschlüsselte Verbindungen, die unabhängig vom tatsächlichen Netzverkehr gleichmäßig ausgelastet werden [Goldberg 1997b].

6.4.1 Onion Routing

Ein Onion-Routing-Netz besteht aus einer Anzahl von als *Onion-Router* bezeichneten Mixen, zwischen denen dauerhafte TCP-Verbindungen bestehen. Ein solches System befindet sich in dem Firewall, der das sichere Netz des Anwenders vom Internet trennt.

Der Zugriff auf das Onion-Routing-Netz erfolgt über *Anwendungs-Proxies,* so daß die Anonymisierung von Proxy-fähigen Anwendungen ohne Modifikation genutzt werden kann. Diese bestehen aus einem anwendungsspezifischen *Client-Proxy* und einem für das Onion-Routing-Protokoll zuständigen *Core-Proxy.* Die anonymisierte Verbindung endet in einem *Responder-Proxy,* der über eine TCP-Verbindung mit dem gewünschten Server kommuniziert.

Der Client-Proxy teilt dem Core-Proxy die Zieladresse mit und leitet Anfragen weiter, wobei er – sofern nicht nur Unbeobachtbarkeit, sondern auch Anonymität erreicht werden soll – identifizierende Daten wie Cookies entfernt. Gegebenenfalls erzeugt er anwendungsspezifische Fehlermeldungen. Client-Proxies existieren für HTTP, ftp, SMTP, ftp und rlogin. Es ist auch möglich, mit einem IP-Tunnel beliebige Internet-Verbindungen zu anonymisieren [Reed 1996].

Der Core-Proxy wählt einen Pfad durch das Onion-Routing-Netz, baut die Verbindung auf und leitet daraufhin die Daten vom Client-Proxy verschlüsselt an das Onion-Routing-Netz weiter.

6.4.1.1 Anonyme Verbindungen

Der Core-Proxy erzeugt eine Verbindungsaufbaunachricht („Onion"), die dem Mix-Protokoll entsprechend mehrfach verschlüsselt wird. Sie enthält für jeden Onion-Router eine Versionsnummer, Bezeichner für die Algorithmen, mit denen die Verbindung in Hin- und Rückrichtung verschlüsselt werden soll, die Adresse des folgenden Onion-Routers (oder 0, um den Responder-Proxy des Onion-Routers zu bezeichnen), die Gültigkeitsdauer der Verbindungsaufbaunachricht sowie einen Wert, aus dem die Sitzungsschlüssel abgeleitet werden. Im ersten Schritt wird zufälliges Padding angehängt; in den folgenden Schritten die für den jeweils nächsten Onion-Router bestimmte Nachricht. In Version 1 des Protokolls werden die ersten 1024 Bit der Nachricht direkt mit RSA verschlüsselt, die weiteren Daten mit DES im OFB-Modus. Die Pfadlänge ist auf 5 festgelegt. Für die Verbindungsverschlüsselung ist neben DES auch RC4 mit 128-Bit-Schlüsseln vorgesehen [Syverson 1997]. Analog zur anonymen Rückadresse kann auch eine *reply onion* erzeugt werden.

Der beim Aufbau gewählte Pfad wird für die Dauer der gesamten Verbindung verwendet.

Ein Onion-Router, der eine Verbindungsaufbaunachricht erhält, entschlüsselt sie und prüft ihre Gültigkeit anhand der angegebenen Gültigkeitsdauer und eines Hash-Wertes, der zur Verhinderung von Replay-Angriffen gespeichert wird. Er erzeugt eine Datenstruktur, in der die ankommende und die ausgehende Verbindung sowie die Verschlüsselungssysteme für beide Richtungen miteinander verknüpft sind. Die Nachricht wird bis zu ihrer ursprünglichen Länge mit zufälligem Padding aufgefüllt und an den nächsten Onion-Router weitergeleitet.

Sobald die anonyme Verbindung besteht, können die mit den in der Verbindungsaufbaunachricht vereinbarten Schlüsseln stromchiffrierten Daten transportiert werden.

6.4.1.2 Verbindung zwischen Onion-Routern

Die Topologie des Netzes ist im voraus definiert. Jeder Onion-Router verfügt über DES-verschlüsselte Verbindungen zu einer festgelegten Menge von *benachbarten* Onion Routern. Über diese Verbindung werden die anonymen Verbindungen sowie Steuerinformationen gemultiplext. Sie werden in *Zellen* fester Größe übertragen. Jede Zelle besteht aus einem für die betreffende dauerhafte Verbindung eindeutigen Bezeichner der anonymen Verbindung *(anonymous connection identifier, ACI)*, der Angabe ihres Typs, der Längenangabe der folgenden Nutzdaten sowie bis zu 44 Bytes Nutzdaten, die mit Padding auf die Maximallänge aufgefüllt werden. Es gibt Zellen der Typen `Padding`, `Create`, `Data` und `Destroy`.

Die Verbindungsaufbaunachrichten werden in `Create`-Zellen transportiert, die Nutzdaten in `Data`-Zellen. Wenn eine Verbindung abbricht, wird eine `Destroy`-Zelle mit der entsprechenden ACI übertragen, die der Empfänger an den folgenden Onion-Router weiterleitet und mit einer weiteren `Destroy`-Zelle bestätigt; die zugehörigen Datenstrukturen werden dann gelöscht. `Padding`-Zellen werden eingefügt, um die Verkehrsanalyse zu erschweren; sie werden vom Empfänger ignoriert. Die Verbindungsverschlüsselung wird für die bereits verschlüsselten Bestandteile der `Create`- und `Data`-Zellen ausgelassen.

Würde die Reihenfolge der ausgehenden `Data`-Zellen der der ankommenden entsprechen, wäre die Zuordnung der Verbindungen für einen Angreifer, der mit den benachbarten Onion-Routern zusammenarbeitet, trivial. Daher wird eine begrenzte Umsortierung vorgenommen: Zellen, die zu einem bestimmten Zeitpunkt von unterschiedlichen Onion-Routern gesendet wurden, können in beliebiger Reihenfolge weiterbearbeitet werden, ohne die Reihenfolge der Daten in einer Verbindung zu zerstören oder die Fairness der Datenvermittlung zu beeinträchtigen. Solange diese Bedingungen erhalten bleiben, können mehrere Zellen einer Verbindung gesammelt und in geänderter Reihenfolge bearbeitet werden. Wenn zwischen interaktiven und nicht zeitkritischen Verbindungen unterschieden wird, bestehen bei letzteren verbesserte Möglichkeiten zur Umsortierung.

6.4.1.3 Sicherheit des Verfahrens

Zusätzlich zu den im einfachen Mix-Netz möglichen Angriffen sind bei Onion Routing einige weitere zu beachten.

Da die Verzögerung durch das Verfahren gering ist, wird die Verbindung zwischen Responder-Proxy und Empfänger nahezu gleichzeitig zur Verbindung zwischen Absender und Onion-Routing-Netz aufgebaut. Damit keine statistische Verkehrsanalyse möglich ist, muß die Kommunikationsverbindung zwischen dem Teilnehmer und seinem lokalen Onion Router also sicher sein, und der lokale Onion Router muß auch fremde Daten transportieren. Eine solche Konfiguration ist in vielen Fällen aber nicht gegeben [Syverson 1997], insbesondere bei Privatanwendern.

Da die dauerhaften Verbindungen verschlüsselt und mit Padding aufgefüllt werden, ist die Verkehrsanalyse für externe Angreifer trotz der kurzen Verzögerungszeiten gegenüber dem einfachen Mix-Netz sogar erschwert. Die Nachbarn eines ehrlichen Onion-Routers können das Padding jedoch erkennen. Die Sicherheit gegen interne Angreifer ist also deutlich geringer. Für Onion-Router ist die Dauer einzelner Verbindungen zu erkennen. Kooperierende Onion-Router am Anfang und Ende einer anonymen Verbindung können die Anonymität daher auch aufdecken, wenn in der Verbindung zusätzlich ehrliche Onion-Router verwendet wurden. Sicherheit gegen diesen Angriff besteht, wenn der erste – definitionsgemäß vertrauenswürdige – Onion-Router ehrliche Nachbarn hat, so daß der Angreifer nicht feststellen kann, woher die Verbindung stammt. Auch in diesem Fall ist die erzielte Konfusion erheblich geringer als im Mix-Netz.

Die in [Syverson 1997] vorgeschlagenen Verschlüsselungsverfahren sind nicht optimal: Um *forward secrecy* zu ermöglichen, sollte entgegen [Syverson 1997] Verbindungsverschlüsselung für alle Zellen eingesetzt werden. Anstelle direkter RSA-Verschlüsselung wäre ein Verfahren wie OAEP [Bellare 1995] zu bevorzugen. Die Schlüsselgröße des verwendeten DES ist mit 56 Bit nicht ausreichend; für langfristige Sicherheit sollten RSA-Schlüssel mit mehr als 1024 Bit verwendet werden können.

Kapitel 7

Zusammenfassung und Ausblick

Um in globalen Netzen das Recht auf informationelle Selbstbestimmung zu gewährleisten, sind technische Verfahren erforderlich, die eine gegenüber Kommunikationspartnern anonyme und gegenüber Dritten unbeobachtbare Nutzung der Netzdienste ermöglichen.

In dieser Arbeit wurden verschiedene Anonymisierungsverfahren untersucht. Mit dem DC-Netz existiert ein sehr sicheres, wenn auch mit hohem Aufwand verbundenes Verfahren, das Anonymität und Unbeobachtbarkeit gewährleistet. Das Mix-Netz ist – sofern es richtig implementiert wird – praktisch sicher und dabei so effizient, daß es im Internet eingesetzt werden kann. Es existieren Implementationen für E-Mail und für interaktive Anwendungen, bei denen für die schnellen Antwortzeiten eine etwas reduzierte Sicherheit in Kauf genommen wird.

Ebenso wie im Internet bestehen auch in anderen Kommunikationsnetzen Datenschutzprobleme. Bei den Betreibern von Mobiltelefonnetzen fällt eine große Menge sensibler Daten an, da sie jeweils die Funkzelle kennen müssen, in der der Nutzer sich aufhält. Um das Erstellen von Bewegungsprofilen zu verhindern, können auf dem Mix-Netz und auf Pseudonymen basierende Verfahren eingesetzt werden [Federrath 1997]. Ob diese Verfahren von Telefonnetzbetreibern in die Praxis umgesetzt werden, ist allerdings fraglich. Im Internet können neue Dienste dagegen mit relativ geringem Aufwand eingeführt werden. Nichtkommerzielle E-Mail-Anonymisierungsdienste (Remailer) werden bereits von Privatpersonen und Organisationen in verschiedenen Staaten betrieben. Hinsichtlich der Anwenderfreundlichkeit sind allerdings noch Verbesserungen erforderlich.

Remailer können – ähnlich wie E-Mail-Verteiler – bei geringen zusätzlichen Kosten in einer vorhandenen Netzinfrastruktur betrieben werden. Für die Anonymisierung von WWW-Zugriffen ist ein deutlich größerer Aufwand erforderlich, da große Datenmengen schnell verarbeitet werden müssen. Ein zuverlässiger Betrieb solcher Dienste ist daher nur kommerziell möglich. *The Anonymizer* hat derzeit 3 000 Kunden, die gegen eine Gebühr von jährlich 60 $ anonym auf WWW-Server zugreifen können [McCullagh 1997]; zusätzlich existiert ein langsamerer freier Zugang. Angesichts der weiterhin bestehenden Datenschutzprobleme kann bei zunehmender Akzeptanz kostenpflichtiger Netzdienste eine deutliche Zunahmei bei den zahlenden Nutzern erwartet werden.

In ähnlicher Weise könnten auch sicherere Anonymisierungsverfahren finanziert werden. Um die Bezahlung des Betreibers sicherzustellen, ohne die Anonymität des Nutzers einzuschränken, müßten Verfahren wie das Mix-Netz mit anonymen digitalen Zahlungsmitteln kombiniert werden. Der geforderte Betrag könnte als anonyme E-Cash-Zahlung mit dem Schlüssel des jeweiligen Mixes verschlüsselt in die Nachricht eingefügt werden. Soll, wie im Internet weit verbreitet, volumenunabhängig abgerechnet werden, kann jeweils der erste Mix die Berechtigung des Nutzers prüfen; die Einnahmen werden dann zwischen den Mixen aufgeteilt.

Solange ein Anonymisierungdienst nicht stark genutzt wird, kann er unter Ausnutzung vorhandener Netzinfrastruktur mit geringem Aufwand betrieben werden; bei starker Nutzung wird eine Finanzierung durch die Nutzer erforderlich. Bei einem Mix-Netz mit sinnvoller Pfadlänge und Padding entsteht im Vergleich zu nicht anonymer Übertragung etwa der zehnfache Aufwand. Da die festen Kosten auf die Nutzer aufgeteilt werden können und die volumenabhängigen Kosten für Internetanbindungen mittlerweile gering sind, können Anonymisierungsdienste zu für die Nutzer akzeptablen Preisen betrieben werden. Eine praktische Umsetzung von Verfahren, die den Datenschutz im Internet sichern können, ist somit möglich.

Literaturverzeichnis

Die nur für die rechtlichen Grundlagen in Kapitel 2 verwendete Literatur wird am Ende dieses Literaturverzeichnisses gesondert aufgeführt.

[anon 1993] an32153@anon.penet.fi: „Dangers of anonymous remailers“. *Risks Forum Digest* 15 (1993) 17. URL: `http://catless.ncl.ac.uk/Risks/15.17.html`

[Atkinson 1995] R. Atkinson: „Security Architecture for the Internet Protocol“. *Internet RFC 1825*, 1995.

[Beaver 1992] D. Beaver: „Foundations of Secure Interactive Computing“. *Advances in Cryptology: Crypto ’91*, Springer, 1992, S. 377–391.

[Bellare 1995] M. Bellare, P. Rogaway: „Optimal Asymmetric Encryption – How to Encrypt with RSA“. *Advances in Cryptology: Eurocrypt ’94*, Springer, 1995, S. 92–111.

[Bellare 1997] M. Bellare, P. Rogaway: „Minimizing the Use of Random Oracles in Authenticated Encryption Schemes“. *Information and Communications Security, ICICS ’97*, Springer, 1997.

[Blome 1996] A. Blome: „Datenschutz im WWW“, 1996. URL: `http://infosoc.informatik.uni-bremen.de/internet/fgtk/OnlineInfos/datenschutz_im_www.html`

[Borchers 1997] D. Borchers: „Angriff der Namenlosen“. *Die Zeit* 37/1997, 5. September 1997.

[Boyan 1997] J. Boyan: „The Anonymizer: Protecting User Privacy on the Web“. *Computer-Mediated Communication Magazine*, 1997. URL: `http://www.december.com/cmc/mag/1997/sep/boyan.html`

[Brauer 1996] E. Brauer, U. van Essen: „Common Criteria: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von IT-

Systemen“. *KES – Zeitschrift für Kommunikations- und EDV-Sicherheit* 12 (1996) 4, S. 48–51.

[Bundestag 1997] Deutscher Bundestag: *Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG),* BT-Drucksache 13/7385, 9. April 1997.

[CC 1996] Common Criteria Editorial Board: „Common Criteria for Information Technology Security Evaluation, Version 1.0“, 1996.

[Chaum 1981] D. Chaum: „Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms“. *Communications of the ACM* 24 (1981) 2, S. 84–88.

[Chaum 1988] D. Chaum: „The Dining Cryptographers Problem. Unconditional Sender and Recipient Untraceability“. *Journal of Cryptology* 1 (1998) 1, S. 65–75.

[Cooper 1995] D. Cooper, A. Birman: „Preserving Privacy in a Network of Mobile Computers“. *1995 IEEE Symposium on Research in Security and Privacy,* IEEE Computer Society Press, 1995, S. 26–38.

[Cottrell 1995] L. Cottrell: „Mixmaster and Remailer Attacks“, 1995. URL: `http://www.obscura.com/~loki/remailer/remailer-essay.html`

[Dai 1995] W. Dai: „Statistical traffic analysis“, 1995. URL: `http://www.eskimo.com/~weidai/traffic.txt`

[Damker 1997] H. Damker, G. Müller: „Verbraucherschutz im Internet“. *Datenschutz und Datensicherheit* 21 (1997) 1, S. 24–29.

[Dusse 1997] S. Dusse et al.: „S/MIME Version 2 Message Specification“, Internet Draft, work in progress, 17. November 1997.

[EFGA 1998] Electronic Frontiers Georgia: Reliable Remailer List, URL: `http://anon.efga.org/anon/rlist.html`

[Federrath 1997] H. Federrath, A. Jerichow, D. Kesdogan, A. Pfitzmann, O. Spaniol: „Mobilkommunikation ohne Bewegungsprofile“. *it+ti* 38 (1996) 4, S. 24–29.

[Franz 1997] E. Franz, A. Jerichow, A. Pfitzmann: „Systematisierung und Modellierung von Mixen“. *Verläßliche IT-Systeme, GI-Fachtagung VIS '97*, Vieweg, 1997, S. 172–190.

[Freier 1996] A. Freier, P. Karlton, P. Kocher: „The SSL Protocol Version 3.0“, 4. März 1996. URL: `ftp://ftp.netscape.com/pub/review/ssl-spec.tar.Z`

[Gabber 1997] E. Gabber et al.: „How to Make Personalized Web Browsing Simple, Secure, and Anonymous“, Bell Labs Technical Memorandum, 1997. URL: `http://www.lpwa.com`. Vorläufige Version in: *Financial Cryptography FC ’97*, Springer, 1997, S. 17ff.

[Goldberg 1997] I. Goldberg, D. Wagner, E. Brewer: „Privacy-enhancing technologies for the Internet“. *IEEE COMPCON 97*, IEEE Computer Society Press, 1997, S. 103–109.

[Goldberg 1997b] I. Goldberg, D. Wagner: „TAZ Servers and the Rewebber Network – Enabling Anonymous Publishing on the World Wide Web“, Project Report, URL: `http://http.cs.berkeley.edu/~daw/cs268/taz.ps`

[Goldreich 1997] O. Goldreich: „The Foundations of Modern Cryptography“, Version 2.2, 1997. URL: `http://theory.lcs.mit.edu/~oded/tfoc.html`. Vorläufige Fassung in: *Crypto ’97*, S. 46–74.

[Goldwasser 1997] S. Goldwasser, M. Bellare: „Lecture Notes on Cryptography“, 19. Juni 1997. URL: `http://www-cse.ucsd.edu/~mihir/papers/gb.ps.gz`

[Gülcü 1996] C. Gülcü, G. Tsudik: „Mixing Email with BABEL“. *1996 Symposium on Network and Distributed System Security*, IEEE Computer Society Press, 1996, S. 2–16.

[Helsingius 1993] J. Helsingius: „The anonymous server anon.penet.fi“, 1993.

[HmbDSB 1996] Der Hamburgische Datenschutzbeauftragte: *15. Tätigkeitsbericht*, 1996.

[Horton 1987] M. Horton: „Standard for Interchange of USENET Messages“. *Internet RFC 1036*, 1987.

[Horton 1994] T. Horton: „Stylometry“. R. Asher (Hrsg.): *The Encyclopedia of Language and Linguistics*, Pergamon Press, 1994, S. 4383–4385.

[ITSEC 1991] Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften: *Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)*, 1991.

[Linn 1993] J. Linn: „Privacy Enhancement for Internet Electronic Mail – Part I: Message Encryption and Authentication Procedures“. *Internet RFC 1421*, 1993.

[Lukat 1991] J. Lukat, A. Pfitzmann, M. Waidner: „Effizientere fail-stop Schlüsselerzeugung für das DC-Netz“. *Datenschutz und Datensicherung*, 15 (1991) 2, S. 71–75.

[Martienssen 1997] M. Martienssen: „Sicherheitsaspekte von Internet-Agenten", Studienarbeit, Universität Hamburg, 1997.

[McCoy 1997] J. McCoy: „Anonymous Networking and Virtual Intranets: Tools for Anonymous Corporations". *Financial Cryptography FC '97*, Springer, 1997, S. 33–37.

[McCullagh 1997] D. McCullagh: „Anonymity At Any Cost". *The Netly News*, 24. November 1997. URL: `http://cgi.pathfinder.com/netly/opinion/0,1042,1594,00.html`

[Menezes 1997] A. Menezes, P. van Oorschot, S. Vanstone: *Handbook of Applied Cryptography*, CRC Press, 1997.

[Micali 1992] S. Micali, P. Rogaway: „Secure Computation". *Advances in Cryptology: Crypto '91*, Springer, 1992, S. 392–404.

[Michels 1996] M. Michels, P. Horster: „Some Remarks on a Receipt-Free and Universally Verifiable Mix-type Voting Scheme". *Advances in Cryptology: Asiacrypt '96*, Springer, 1996, S. 125–132.

[Newman 1996] R. Newman: „The Church of Scientology vs. anon.penet.fi", 1996. URL: `http://www2.thecia.net/users/rnewman/scientology/home.html`

[Pfitzmann 1989] A. Pfitzmann, B. Pfitzmann, M. Waidner: „Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2*64+16)-kbit/s-Teilnehmeranschluß". *Datenschutz und Datensicherung*, 13 (1989) 12, S. 605–622.

[Pfitzmann 1990] A. Pfitzmann: *Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz*, Springer, 1990.

[Pfitzmann 1990b] B. Pfitzmann, A. Pfitzmann: „How to Break the Direct RSA-Implementation of MIXes". *Advances in Cryptology: Eurocrypt '89*, Springer, 1990, S. 373–381.

[Pfitzmann 1991] B. Pfitzmann, M. Waidner: „Unbedingte Unbeobachtbarkeit mit kryptographischer Robustheit". *VIS '91 Verläßliche Informationssysteme*, Spriger, 1991, S. 302–320.

[Rackoff 1993] C. Rackoff, D. Simon: „Cryptographic Defense Against Traffic Analysis". *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing (STOC)*, ACM Press, 1993, S. 672–681.

[Rannenberg 1995] K. Rannenberg et al.: „Mehrseitige Sicherheit als integrale Eigenschaft von Kommunikationstechnik". H. Kubicek et al. (Hrsg.): *Jahrbuch Telekommunikation und Gesellschaft 1995*, v. Decker, 1995, S. 254–260.

[Rannenberg 1996] K. Rannenberg, A. Pfitzmann, G. Müller: „Sicherheit, insbesondere mehrseitige IT-Sicherheit“. *it+ti – Informationstechnik und Technische Informatik* 38 (1996) 4, S. 7–10.

[Reed 1996] M. Reed, G. Syverson, D. Goldschlag: „Proxies for Anonymous Routing“. *12th Annual Computer Security Applications Conference,* IEEE Computer Society Press, 1996, S. 95–104.

[Reiter 1997] M. Reiter, A. Rubin: „Crowds: Anonymity for Web Transactions“, DIMACS Technical Report 97-15, 1997.

[Rossum 1995] H. van Rossum et al.: *Privacy-Enhancing Technologies: The Path to Anonymity,* Registratiekamer; Information and Privacy Commissioner / Ontario, 1995.

[RSA 1993] RSA Laboratories: „PKCS #1: RSA Encryption Standard“, Version 1.5, 1993.

[Sako 1995] K. Sako, J. Kilian: „Receipt-Free Mix-Type Voting Scheme“. *Advances in Cryptology: Eurocrypt ’95*, Springer, 1995, S. 393–403.

[Schaar 1996] P. Schaar: „Datenschutzfreier Raum Internet?“ *Computer und Recht* 12 (1996) 3, S. 170–177.

[Schneier 1996] B. Schneier: *Applied Cryptography,* 2. Auflage, Wiley, 1996.

[Syverson 1997] P. Syverson, D. Goldschlag, M. Reed: „Anonymous Connections and Onion Routing“. *IEEE Symposium on Security and Privacy,* IEEE Computer Society Press, 1997, S. 44–54.

[Tanenbaum 1989] A. Tanenbaum: *Computer Networks*, 2. Auflage, Prentice Hall, 1989.

[Wagner 1996] D. Wagner, B. Schneier: „Analysis of the SSL 3.0 protocol“. *The Second USENIX Workshop on Electronic Commerce,* USENIX Press, 1996, S. 29–40.

[Waidner 1990] M. Waidner: „Unconditional Sender and Recipient Untraceability in spite of Active Attacks“. *Advances in Cryptology: Eurocrypt ’89*, Springer, 1990, S. 302–319.

[Wayner 1996] P. Wayner: *Disappearing Cryptography,* AP Professional, 1996.

[Ylönen 1997] T. Ylönen, T. Kivinen, M. Saarinen: „SSH Transport Layer Protocol“, Internet Draft, work in progress, 7. November 1997.

[Zimmermann 1995] P. Zimmermann: *The Official PGP User’s Guide*, MIT Press, 1995.

Literatur zu Kapitel 2:

[Abelson 1997] H. Abelson et al.: „The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption“. *World Wide Web Journal* 2 (1997) 3, S. 241–257.

[BfD 1997] Der Bundesbeauftragte für Datenschutz: *16. Tätigkeitsbericht*, 1997.

[Bizer 1995] J. Bizer: „Rechtsprobleme der Vertraulichkeit elektronischer Kommunikation“. *Trust Center – Grundlagen, rechtliche Aspekte, Standardisierung und Realisierung*, Vieweg, 1995, S. 213–225.

[Bizer 1997] J. Bizer: „Veranstaltungsbesprechung – 6. Wiesbadener Forum Datenschutz: Datenschutz durch Kryptographie?“ *Datenschutz und Datensicherheit* 21 (1997) 8, S. 496–497.

[Budapest 1996] Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation: *Budapest-Berlin Memorandum, Datenschutz und Privatsphäre im Internet – Bericht und Empfehlungen*, 19. April 1996.

[Bundesrat 1997] *Begründung zum Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag)*, Hbg. BüScha-Dr. 15/7297, 1997.

[BVerfG 1983] Bundesverfassungsgericht: Urteil vom 15. Dezember 1983, *BVerfGE* 65, 1.

[BVerfG 1992] Bundesverfassungsgericht: Beschluß vom 25. März 1992, *BVerfGE* 85, 386.

[Dammann 1992] Dammann in Simitis/Dammann/Mallmann/Reh: *Kommentar zum Bundesdatenschutzgesetz*, 4. Aufl., Nomos, 1992.

[Dean 1996] D. Dean, E. Felten, D. Wallach: „Java Security: From HotJava to Netscape and Beyond“. *1996 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, 1996.

[Detweiler 1993] L. Detweiler: „Anonymity on the Internet“, 1993. URL: `http://www.intac.com/man/faq/net-anonymity`

[Dillon 1996] J. Dillon: „Are The FEDS Sniffing your Re-mail?“ *Covert Action Quarterly* 56/1996.

[Eklund 1996] E. Eklund: „Controlling and Securing Personal Privacy and Anonymity in the Information Society“, Hut Network Seminar ’95, 1996. URL: `http://www.tcm.hut.fi/Opinnot/Tik-110.501/1995/privacy.html`

[Ellerman 1997] C. Ellerman: „Channel Definition Format (CDF)“, Version 1.0, 30. September 1997. URL: `http://www.microsoft.com/standards/cdf.htm`

[Engel 1996] C. Engel: „Inhaltskontrolle im Internet“. *AfP Zeitschrift für Medien- und Kommunikationsrecht* 27 (1996) 3, S. 220–227.

[Engel-Flechsig 1997] S. Engel-Flechsig: „IuKDG vom Bundestag verabschiedet“. *Datenschutz und Datensicherheit* 21 (1997) 8, S. 474–476.

[Etzioni 1996] O. Etzioni: „The World Wide Web: quagmire or gold mine?“ *Communications of the ACM* 39 (1996) 11, S. 65–68.

[EU-Komm. 1996] Europäische Kommission: *Illegale und schädigende Inhalte im Internet* – Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß sowie den Ausschuß der Regionen vom 16. Oktober 1996, COM (96) 487.

[EU-Parl. 1997] Europäisches Parlament: *Entschließung* vom 24. Juli 1997, KOM (96) 487 - C4-0592/96.

[Froomkin 1996] M. Froomkin: „Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases“. *U. Pittsburg Journal of Law and Commerce* 15 (1996), S. 395ff.

[Geogia 1997] United States District Court, Northern District of Georgia: *American Civil Liberties Union of Georgia, et al., v. Zell Miller et al.*, 1997.

[Hamm 1997] R. Hamm: „Kryptokontroverse“. *Datenschutz und Datensicherheit* 21 (1997) 4, S. 186–191.

[Hannaford 1996] C. Hannaford: „Anonymous re-mailers“. Royal Canadian Mounted Police (Hrsg.): *Technological Crime Bulletin* 2 (1996) 2.

[Helmers 1997] S. Helmers: „Freie Rede im Schutz der Maske“. *Spiegel Online* 14/1997. URL: `http://www.spiegel.de/arc/oworld/97/14/sonv04.html`

[Hermes 1996] G. Hermes: Kommentierung zu Art. 10 GG. In H. Dreier (Hrsg.): *Grundgesetz: Kommentar*, Mohr, 1996.

[Huhn 1997] M. Huhn, A. Pfitzmann: „Technische Randbedingungen jeder Kryptoregulierung“. G. Müller, A. Pfitzmann (Hrsg.): *Mehrseitige Sicherheit*, Addison-Wesley-Longman, 1997.

[IuKDG 1997] *Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG)* vom 22. Juli 1997, BGBl. I 1997 S. 1870–1880.

[Johns 1993] M. Johns: „Identification Protocol“. *Internet RFC 1413*, 1993.

[KES 1997] „5. Deutscher IT-Sicherheits-Kongress: Der Rückblick“. *KES – Zeitschrift für Kommunikations- und EDV-Sicherheit* 13 (1997) 3, S. 44–54.

[Koke 1997] A. Koke: „Java und ActiveX – Gefahr aus dem Internet?“ *Mit Sicherheit in die Informationsgesellschaft*, Tagungsband 5. Deutscher IT-Sicherheitskongreß des BSI, SecuMedia, 1997.

[Kristol 1997] D. Kristol, L. Montulli: „HTTP State Management Mechanism“. *Internet RFC 2109*, 1997.

[Krüger 1996] H. Krüger: Kommentierung zu Art. 10 GG. In M. Sachs (Hrsg.): *Grundgesetz: Kommentar*, Beck, 1996.

[Kubicek 1996] H. Kubicek: „Das Netz weiß zuviel“. Interview. *die tageszeitung*, 4. April 1996, S. 12.

[LAB 1997] European Commission Legal Advisory Board: *Response to the Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services*, 1997. URL: `http://www2.echo.lu/legal/en/internet/gplabreply.html`

[Laufhütte 1987] H. Laufhütte in G. Pfeiffer (Hrsg.): *Karlsruher Kommentar zur Strafprozeßordnung*, Beck, 1987.

[Lee 1996] G. Lee: „Addressing Anonymous Messages in Cyberspace“. *Journal of Computer-Mediated Communication* 2 (1996) 1. URL: `http://www.usc.edu/dept/annenberg/vol2/issue1/anon.html`

[Löffler 1983] M. Löffler: *Presserecht – Kommentar*, Beck, 1983.

[Löffler 1994] M. Löffler, R. Pricker: *Handbuch des Presserechts*, Beck, 1994.

[Mayer 1997] P. Mayer: „FAQ: Multimedia-Gesetzgebung – ISP“, 1997. URL: `http://www.tuebingen.netsurf.de/~pmayer/faq.htm`

[MDStV 1997] *Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag)*, Hamburgisches Gesetz zum Mediendienste-Staatsvertrag, 25. Juni 1997, Hamburgisches Gesetz- und Verordnungsblatt 1997, S. 253–260.

[NIST 1996] National Institute of Standards and Technology: „The World Wide Web: Managing Security Risks“. *NIST ITL Bulletin*, Mai 1996.

[Nitsch 1995] P. Nitsch: „Datenschutz und Informationsgesellschaft“. *Zeitschrift für Rechtspolitik* 28 (1995) 10, S. 361–363.

[Postel 1981] J. Postel: „Internet Protocol“. *Internet RFC 791*, 1981.

[Postel 1981b] J. Postel: „Transmission Control Protocol“. *Internet RFC 793*, 1981.

[Quittner 1995] J. Quittner: „Unmasked on the Net“. *Time Magazine* 9/1995.

[Rat 1995] Der Rat für Forschung, Technologie und Innovation: *Informationsgesellschaft: Chancen, Innovationen und Herausforderungen*, Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie (Hrsg.), 1995.

[Rexrodt 1997] G. Rexrodt, M. Bangemann: „Themenpapier zur Europäischen Ministerkonferenz Globale Informationsnetze“, 1997. URL: `http://www2.echo.lu/bonn/`

[Roßnagel 1997] A. Roßnagel: „Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger“. *Zeitschrift für Rechtspolitik* 30 (1997) 1, S. 26–30.

[Roßnagel 1997b] A. Roßnagel: *Schriftliche Stellungnahme zu den Fragen des Bundestags-Ausschusses für Bildung, Wissenschaft, Forschung, Technologie und Technikfolgenabschätzung zur Vorbereitung der öffentlichen Anhörung zum Informations- und Kommunikationsdienste-Gesetz*, Ausschuß-Drucks. 13-615e, 5. Mai 1997.

[Schallbruch 1995] M. Schallbruch: „Electronic Mail im Internet – Wie steht es mit dem Datenschutz?“ *Datenschutz-Nachrichten* 18 (1995) 5, S. 11–15.

[Schweighofer 1997] E. Schweighofer: „Data Mining und Datenschutz am Beispiel Österreichs“. *Datenschutz und Datensicherheit* 21 (1997) 8, S. 458–461.

[Seltzer 1995] R. Seltzer: „Anonymity for fun and deception: The other side of ‘community’“, 1995. URL: `http://www.samizdat.com/anon.html`

[Simitis 1992] S. Simitis in Simitis/Dammann/Mallmann/Reh: *Kommentar zum Bundesdatenschutzgesetz*, 4. Auflage, Nomos, 1992.

[Simitis 1997] S. Simitis: „Daten- oder Tatenschutz – Streit ohne Ende?“ *Neue Juristische Wochenschrift* 50 (1997) 29, S. 1902f.

[Strassmann 1996] P. Strassmann, W. Marlow: „Risk-Free Access Into The Global Information Infrastructure Via Anonymous Re-Mailers“, 1996. URL: `http://www.strassmann.com/pubs/anon-remail.html`

[Ulfelder 1996] S. Ulfelder: „Online snoop!“ *Computerworld*, 12. August 1996.

[USSC 1960] U.S. Supreme Court: *Talley v. California*, 362 U.S. 60.

[WiB 1997] Pressezentrum des deutschen Bundestages (Hrsg.): „Forschung: Vor Schaden durch Kryptogesetz gewarnt“. *Woche im Bundestag* 9/1997.

[WP 1996] Working Party on illegal and harmful content on the Internet: *Report*, 28. November 1996. URL: `http://www2.echo.lu/legal/en/internet/content/wpen.html`

[Zimmerman 1991] D. Zimmerman: „The Finger User Information Protocol“. *Internet RFC 1288*, 1991.